UNIVERSITA` DEGLI STUDI DI PISA

Dipartimento di Economia e Management

Corso di laurea magistrale in Banca, Borsa e Assicurazioni

TESI DI LAUREA:

IL SISTEMA DEI CONTROLLI INTERNI IN BANCA: PRINCIPALI ASPETTI DEL NUOVO QUADRO DI RIFERIMENTO

RELATORE

Prof.ssa Paola **FERRETTI**

CANDIDATO

Sara **CRISALLI**

Anno accademico 2013-2014

Indice degli argomenti

Introduzione

La crisi ha evidenziato come il combinato di carenze nello strumentario del risk management, distorsioni nei sistemi di remunerazione nonché inadeguatezze della governance abbia determinato un circolo vizioso che ha portato le banche all'assunzione di rischi sempre crescenti.
La governnace e il sistema dei controlli interni degli intermediari finanziari sono dall'inizio al centro del dibattito, giacché è ormai pacifica la convinzione che lacune e inefficienze riscontrate in questi ambiti hanno contribuito a determinare la situazione di crisi o a ritardare l'adozione di tempestive misure correttive. Eppure, negli anni precedenti la crisi vi era un ampio consenso sul fatto che l'assetto del sistema finanziario e quello di gran parte, se non di tutti, gli intermediari fosse tale da assicurare la stabilità.
Non si può negare, a fronte di queste circostanze, che anche la regolamentazione e il controllo da parte delle autorità competenti siano stati, quanto meno in taluni casi, inadeguati. Si evidenziò così l'esigenza di regolamentare nuovamente la governance e il sistema dei controlli interni delle banche, facendo tesoro delle lezioni della crisi per rimediare agli elementi di debolezza riscontrati.

La presente trattazione si riferisce in maniera specifica alla revisione delle disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni, operata dalla Banca d'Italia nel luglio 2013, ponendosi l'obiettivo di fornire gli elementi necessari per comprendere portata e impatto della nuova normativa di riferimento.

L'articolazione della tesi prevede la suddivisione in quattro capitoli.
Nel primo capitolo, intitolato "*Le nuove disposizioni di vigilanza prudenziale in materia di controlli interni e di governance*", viene fornito l'inventario delle disposizioni e degli interventi che hanno riguardato il tema del controllo interno in banca e, più in generale, della governance bancaria. Viene inoltre introdotta la nuova disciplina, evidenziandone finalità, principi di fondo e generali.

Il secondo capitolo, intitolato "*Il sistema dei controlli interni: le principali novità del nuovo framework regolamentare*", descrive gli elementi innovativi introdotti dal nuovo quadro di riferimento, accorpandoli in due categorie. Vengono, infatti, trattati, nella prima parte del capitolo, gli aspetti innovativi riferibili al tema della governance interna, per poi dedicare la seconda parte alle novità attinenti il controllo dei rischi.

Il terzo capitolo, intitolato "*La procedura di consultazione e le disposizioni transitorie*", approfondisce le risposte fornite dal sistema bancario ai quesiti posti dalla Banca d'Italia in relazione a particolari aspetti delle nuove disposizioni, e evidenzia alcune delle osservazioni alla disciplina avanzate dai rispondenti alla procedura di consultazione. Riassume, altresì, le principali scadenze del regime transitorio, concentrandosi, in particolare, su quella del 31 gennaio 2014, entro la quale le banche sono state chiamate a inviare all'Autorità di Vigilanza la relazione sulla gap analysis condotta sulle proprie strutture di controllo interno.

L'ultimo capitolo, rubricato "*Unicredit, UBI Banca e Banca Popolare di Sondrio: sistemi di controllo interno a confronto*", presenta l'architettura dei controlli interni dei tre istituti bancari italiani citati nel titolo. La scelta degli istituti è stata guidata dalla classifica redatta da RiskGovernnace, centro di ricerca, informazione e consulenza in ambito di Risk Management & Corporate Governance del Politecnico di Milano. L'intento del capitolo conclusivo è quello di delineare il sistema dei controlli interni di Unicredit, prima banca italiana in classifica, di UBI Banca che ha occupato, invece, la posizioni intermedia tra le italiane, e infine di Banca Popolare di Sondrio, ultima tra le domestiche.

CAPITOLO 1

Le nuove disposizioni di vigilanza prudenziale per le banche in materia di controlli interni e di governance

1.1 Profili evolutivi della disciplina di vigilanza in materia di controlli interni

Il quadro normativo internazionale, comunitario e nazionale si è considerevolmente sviluppato negli ultimi anni, in ragione dell'ampliamento delle attività svolte dalla banca.
Ai fini della comprensione delle vigenti disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni[1] appare opportuno offrire, nel prosieguo di questo paragrafo, un inventario delle disposizioni che hanno avuto un considerevole impatto in materia.

Nel quadro di una costante azione tesa a rafforzare la supervisione prudenziale, allontanandosi sempre più da un modello di vigilanza di tipo strutturale, il Comitato di Basilea, che fino a quel momento aveva trattato i controlli interni in relazione a specifici aspetti dell'attività bancaria, ha emanato nel 1998 lo *Schema per i sistemi di controllo interno nelle organizzazioni bancarie*.
Grazie a questo documento viene presentato un vero e proprio sistema dei controlli che si estende a tutte le operazioni bancarie, ipotizzando parallelamente uno schema di principi ad uso delle Autorità di vigilanza per una esaustiva e corretta valutazione dell'intermediario.
Viene acquisita dalla comunità finanziaria l'idea che un sistema di efficaci controlli interni costituisce elemento essenziale della gestione bancaria e uno dei principali criteri di valutazione a disposizione della Vigilanza. Il Comitato consacra il canone secondo cui rigorosi controlli interni contribuiscono alla realizzazione delle finalità aziendali e al mantenimento della stabilità del sistema. Dal quel momento in poi in ogni intervento del Comitato sui temi del rischio sarà ribadito l'insegnamento per cui il sistema dei controlli favorisce il conseguimento degli obiettivi strategici, la conformità alle norme, la riduzione del rischio di perdite impreviste o di eventi pregiudizievoli alla reputazione dell'azienda.

Il Comitato di Basilea nel documento del 1998 riprende i caratteri fondamentali del sistema dei controlli interni indicati nel *CoSo Report*[2]. La prima definizione di controllo interno, nonché una delle più accreditate, è stata, infatti, fornita dal CoSo Report, autorevole esempio di best practices sviluppate nel settore privato che, mediante atti prodotti da organismi internazionali, hanno ingresso nella legislazione settoriale.
La definizione riportata nel Coso Report identifica il controllo interno nel "processo, svolto dal consiglio di amministrazione, dai dirigenti e da altri operatori della struttura aziendale, che si prefigge di fornire una ragionevole sicurezza sulla realizzazione degli obiettivi rientranti nelle seguenti categorie:

- efficacia ed efficienza delle attività operative;
- attendibilità delle informazioni di bilancio;
- conformità alle leggi e ai regolamenti in vigore"[3].

Appare chiaro, sin da subito, come il controllo interno sia uno strumento al servizio del management per il raggiungimento degli obiettivi prefissati, in grado di fornire la ragionevole certezza della correttezza nella gestione secondo i canoni di efficacia ed efficienza, di attendibilità dei dati contenuti nel bilancio e di svolgimento dell'attività conformemente alle normative ed ai regolamenti ai quali l'azienda bancaria è sottoposta.

---

[1] Il 2 luglio 2013, la Banca d'Italia ha pubblicato il 15° aggiornamento alla Circolare n. 263 del 27/12/2006, *Nuove disposizioni di vigilanza prudenziale per le banche*, inserendo nel Titolo V i seguenti capitoli: il Capitolo 7 "Il sistema dei controlli interni", il Capitolo 8 "Il sistema informativo" e il Capitolo 9 "La continuità operativa".
[2] Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control. Integrated Framework*, New York, dicembre 1992, disponibile in traduzione italiana a cura di PricewaterhouseCoopers, *Il sistema di controllo interno*, Milano, 2004, contenente il "Progetto corporate governance per l'Italia".
[3] *Ibid*.

Lo standard di riferimento descritto nel CoSo Report è stato successivamente ampliato e diffuso con la denominazione di *ERM – Enterprise Risk Management*[4]. L'ERM viene proposto come modello che sviluppa le linee del CoSo Report e, pur non sostituendosi ad esso, di fatto tende a incorporarlo per realizzare un unico e più aggiornato standard di riferimento, focalizzando maggiormente l'attenzione sulla gestione del rischio. Il framework fornito dalla Treadway Commission altro non è che la struttura portante, l'impalcatura concettuale del sistema dei controlli[5].

Ispirandosi a quanto indicato dal CoSo Report, il Comitato di Basilea ha fornito una definizione analoga rintracciabile nel documento pubblicato nel 1998[6]. In esso si legge che il controllo interno è un processo posto in essere dal consiglio di amministrazione, dall'alta direzione e da tutti i livelli del personale, che non consiste unicamente in una procedura o in una politica applicata in un dato momento, bensì opera costantemente a tutti i livelli all'interno della banca. Sebbene competa al Consiglio di amministrazione e all'Alta direzione la responsabilità di instaurare una cultura che favorisca un efficace processo di controllo interno e di sorvegliarne l'efficacia in modo continuativo, a questo processo deve partecipare ogni individuo che opera nell'organizzazione al fine di perseguire i seguenti obiettivi:

1. efficienza ed efficacia delle attività (obiettivi di performance);
2. affidabilità, completezza e tempestività dei rendiconti finanziari e di gestione (obiettivi di informazione);
3. conformità con le leggi e le regolamentazioni applicabili (obiettivi di conformità).

Con l'emanazione da parte della Banca d'Italia delle *Istruzioni di vigilanza per le banche*[7], sono state adattate all'ordinamento italiano le linee guida del Comitato di Basilea, conferendo al modello di derivazione anglosassone una chiara valenza organizzativa e dando maggior risalto all'obiettivo di protezione dalle perdite.
In definitiva il sistema dei controlli interni divenne fondamentale requisito di carattere qualitativo che l'intermediario doveva possedere.
Le Istruzioni di vigilanza recepivano così l'impostazione del Comitato di Basilea, consolidando il principio in base al quale il sistema dei controlli interni è parte integrante dell'attività di impresa, finalizzato al corretto governo dei rischi come un vero e proprio ombrello protettivo della gestione nel suo complesso.

Nel 1999 il Comitato di Basilea ha avviato un processo di revisione dello schema di adeguatezza patrimoniale che si è concluso con l'approvazione nel 2004 del *Nuovo accordo sul capitale*, detto Basilea 2, introdotto in ambito europeo attraverso la Direttiva CRD. Quest'ultima è stata recepita a livello nazionale con l'emanazione da parte della Banca d'Italia delle *Nuove disposizioni di vigilanza prudenziale per le banche*[8], nelle quali quasi niente è stato modificato della definizione del sistema dei controlli interni già fornita nel 1999, salvo sottolineare l'importanza degli aspetti organizzativi che interessano i controlli interni e la stretta connessione tra questi e i controlli interni.

Il Comitato di Basilea nell'aprile 2005 ha emanato le linee guida in tema di compliance[9], per uniformare le disposizioni in materia di vigilanza bancaria sulla gestione del rischio di non conformità alle norme ed incentivare l'introduzione di migliori prassi volte a prevenire la violazione di leggi, regolamenti e standard di condotta.

---

[4] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management. Integrated Framework: Executive Summary and Framework*, New York, settembre 2004, disponibile in traduzione italiana a cura di Associazione Italiana Internal Auditors e PricewaterhouseCoopers, *La gestione del rischio aziendale*, Milano, 2006.
[5] Si consenta il rinvio a Dellarosa E., Razzante R., *Il nuovo sistema dei controlli interni della banca*, Milano, Franco Angeli, 2010.
[6] Comitato di Basilea, *Schema per i sistemi di controllo interno nelle organizzazioni bancarie*, Basilea, settembre 1998.
[7] Banca d'Italia, *Istruzioni di vigilanza per le banche*, *Circ. n. 229 del 21/4/1999*, Tit. IV, Cap. 11.
[8] Banca d'Italia, *Nuove disposizioni di vigilanza prudenziale per le banche*, *Circ. n. 263 del 27/12/2006*.
[9] Comitato di Basilea, *Compliance and the compliance function in banks*, Basilea, aprile 2005.

I principi del Comitato sono stati successivamente recepiti dalla Banca d'Italia attraverso l'emanazione, nel luglio 2007, delle disposizioni di vigilanza rubricate *La funzione di conformità (compliance)*, per mezzo delle quali è stata formalmente introdotta la funzione di compliance nel sistema dei controlli interni degli istituti bancari nazionali, adattando le più generali previsioni del Comitato di Basilea alla realtà italiana.

Inoltre la materia è stata trattata a livello comunitario dalla direttiva 2004/39/CE o *MiFID* (Market in financial instrument directive) e dalle connesse misure di attuazione, contenute nella Direttiva 2006/73/CE e nel Regolamento 2006/1287/CE.
Ai fini della nostra analisi, il cambiamento più significativo apportato dalla MiFID si rintraccia nelle norme dedicate ai requisiti organizzativi dell'intermediario. Viene evidenziata la necessità di dotarsi di procedure amministrativo-contabili appropriate, di efficaci meccanismi di controllo interno, di efficienti politiche di gestione dei conflitti d'interesse.
Le disposizioni sulle materie organizzative e procedurali sono state recepite in Italia con la normazione congiunta di Banca d'Italia e Consob[10], situandosi nel crocevia di competenze e rivestendo grande importanza ai fini di vigilanza prudenziale.

Sul fronte della governance è ormai assunto pienamente condiviso che controlli e governo societario siano aspetti solo apparentemente distinti, che in realtà si integrano e concorrono insieme al buon funzionamento dell'impresa e sono fondamentali per perseguire una duratura creazione di valore, aumentare la fiducia degli investitori e assicurare al contempo una sana crescita economica[11].
L'esperienza della crisi finanziaria, scaturita nell'autunno del 2007 ed esplosa nel 2008, ha messo in luce con un'enfasi ancora maggiore rispetto al passato la crucialità della corporate governance[12] e dei sistemi di controllo ai fini del presidio della stabilità aziendale e della capacità delle banche di assorbire i rischi connessi con mutamenti di scenario e con gli effetti di operazioni complesse.
In buona parte, le carenze nei modelli e nei processi organizzativi e di controllo sono state identificate, se non come il fattore scatenante della crisi, come una determinante cruciale della stessa.
Anche il dibattito internazionale è stato particolarmente intenso negli ultimi anni alla luce della crisi finanziaria[13]. Nel complesso, è emerso il diffuso consenso sugli effetti che eventuali carenze nel sistema dei controlli degli intermediari finanziari possono determinare sulla loro buona gestione e, conseguentemente, sulla loro stabilità e su quella del sistema finanziario[14].

---

[10] Consob e Banca d'Italia, *Regolamento della Banca d'Italia e della Consob ai sensi dell'art. 6 comma 2-bis del Testo unico della finanza*, altrimenti detto *Regolamento Congiunto*, 2007.

[11] Cfr. Tarantola A. M., *Il sistema dei controlli interni nella governance bancaria,* intervento al Convegno DEXIA Crediop 4° Incontro Compliance, "Il sistema dei controlli aziendali: alla ricerca di una governance", Roma, 6 giugno 2008.

[12] Sul tema della corporate governance, sono intervenuti, tra gli altri, l'allora Direttore Generale della Banca d'Italia, Fabrizio Saccomanni, con l'intervento di chiusura del convegno "Il governo societario e la sana e prudente gestione delle banche" del 25 settembre 2012 e l'allora Direttore Centrale per la Vigilanza Bancaria e Finanziaria, Stefano Mieli, con l'intervento *Sistemi di controllo dei rischi e governo degli intermediari: una prospettiva di vigilanza* al convegno ADEIMF del 3 febbraio 2012, "Corporate governance e gestione dei rischi: gli insegnamenti della crisi".

[13] Sull'importanza dei controlli interni si è espresso più volte il CEBS/EBA: nel 2006, con il documento del 25 gennaio 2006, *Guidelines on the Application of the Supervisory Rewiew Process under Pillar 2*, e con il documento del 14 dicembre 2006, *Guidelines on outsourcing*, e, nel 2011, con le *Guidelines on Internal Governance*, 27 settembre 2011, su cui si soffermeremo nel prosieguo del paragrafo. Anche il Comitato di Basilea ha disciplinato sia aspetti specifici (*Fair value measurement and modelling: An assessment of challenges and lessons learned from market stress*, giugno 2008; *The internal audit function in banks*, giugno 2012) sia principi generali (*Principles for enhancing corporate governance*, ottobre 2010; *Core Principles for Effective Banking Supervision*, settembre 2012).

[14] Cfr. Banca d'Italia, *Disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni, sistema informativo e continuità operativa. Relazione sull'analisi d'impatto*, giugno 2013.

Le carenze individuate hanno condotto l'EBA (Autorità Bancaria Europea) a pubblicare, nel settembre 2011, le nuove *Linee guida in materia di Internal Governance*[15], volte a migliorare la corretta attuazione degli assetti di governo e di controllo interno delle banche.
Le EBA Guidelines dedicano particolare attenzione al tema del governo interno delle banche e definiscono i criteri per assicurare la presenza di organi aziendali e di funzioni di controllo interno efficienti. Tra le principali innovazioni, sono stati introdotti principi e riferimenti ai compiti delle funzioni di controllo, e in particolare al ruolo centrale e strategico del responsabile del Risk Management e della funzione di controllo dei rischi.

Lo scorso 5 gennaio 2012 la Banca d'Italia ha pubblicato una *Comunicazione*[16] in materia di corporate governance delle banche, recante alcune norme di attuazione delle *Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*[17] del 4 marzo 2008, come integrate dalla precedente *Nota di chiarimenti*[18] del 19 febbraio 2009.
Le disposizioni del 2008, che fanno seguito a una approfondita consultazione avviata nell'ottobre 2007, delineano un quadro normativo organico e integrato con gli interventi del periodo che attribuivano all'organizzazione un ruolo centrale nella definizione delle strategie aziendali e delle politiche di gestione e controllo dei rischi tipici dell'attività bancaria[19].
Nella prospettiva di rafforzare gli standard minimi di organizzazione e governo societario di tutti gli intermediari, i principi indicati riguardano: la chiara distinzione dei ruoli e delle responsabilità, l'appropriato bilanciamento dei poteri, l'equilibrata composizione degli organi, l'efficacia dei controlli, il presidio di tutti i rischi aziendali, l'adeguatezza dei flussi informativi.
Le norme rimettono in generale all'autonomia degli intermediari il compito di individuare gli assetti di governo più rispondenti alle caratteristiche dimensionali, strutturali e operative, secondo il criterio guida della proporzionalità.
La disciplina, infatti, non fa riferimento a organi aziendali nominativamente individuati, in quanto variabili in relazione al modello di corporate governance o di amministrazione e controllo prescelto, ma richiama le funzioni di supervisione strategica, di gestione e di controllo che devono essere ripartite tra gli organi aziendali o all'interno di essi. Tralasciando in questa sede l'inquadramento delle tre funzioni, pare opportuno segnalare che le disposizioni del 2008 specificano che più funzioni possono essere svolte dallo stesso organo o più organi possono condividere la stessa funzione.

Più di recente il Financial Stability Board si è soffermato sul tema dei controlli interni nell'ambito del peer review report *Thematic review on risk governance* del 12 febbraio 2013. Il documento, sulla base dei contributi delle banche intervistate e delle autorità di supervisione, offre un importante contributo in quanto: identifica i principali sviluppi in materia di governance registrati negli ultimi anni, i progressi e le aree che necessitano di ulteriore miglioramento; definisce le caratteristiche delle funzioni chiave nell'ambito della risk governance, alla luce delle best practices riscontrate; formula raccomandazioni per le autorità di supervisione e per gli standard setters rilevanti al fine di promuovere una più efficace e solida risk governance degli intermediari[20].

[15] EBA, *Guidelines on Internal Governance*, settembre 2011.
[16] Banca d'Italia, *Applicazione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, 11 gennaio 2012.
[17] Banca d'Italia, *Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, 4 marzo 2008.
[18] Banca d'Italia, *Nota di chiarimenti in materia di governance*, 19 febbraio 2009, attraverso la quale Banca d'Italia fornisce chiarimenti di carattere operativo volti ad agevolare una corretta applicazione, da parte delle banche e dei gruppi bancari, delle *Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, il cui termine per l'attuazione risale al 30 giugno 2009.
[19] Cfr. Banca d'Italia, *Comunicato stampa* del 4 marzo 2008.
[20] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.

Nel panorama degli interventi normativi che si sono occupati di sistema dei controlli interni e più in generale di organizzazione, merita un breve cenno anche l'attuazione in ambito europeo dell'accordo di Basilea 3, avvenuta grazie all'emanazione di due atti normativi datati 26 giugno 2013: il Regolamento UE n. 575/2013 (Capital Requirement Regulation - CRR) e la Direttiva 2013/36/UE (Capital Requirement Directive IV - CRD IV), con i quali vengono introdotte nell'Unione europea le regole definite con Basilea 3, con l'intento di promuovere un sistema bancario più solido e resistente agli shock finanziari.
Tali nuovi provvedimenti, che sostituiscono integralmente la Direttiva CRD e le sue successive modificazioni, costituiscono il quadro normativo di riferimento nell'Unione europea per banche e imprese di investimento dal 1° gennaio 2014.
A livello nazionale, con il comunicato stampa del 19 dicembre 2013, la Banca d'Italia ha comunicato l'emanazione della Circolare n. 285 del 17 dicembre 2013, *Disposizioni di vigilanza per le banche*, con cui si è dato avvio all'attuazione in Italia della Direttiva CRD IV. Le nuove disposizioni sono entrate in vigore il 1° gennaio 2014, data in cui è divenuto direttamente applicabile anche il Regolamento CRR in materia di requisiti patrimoniali.

La necessità di calare gli orientamenti delle istituzioni comunitarie e degli organismi internazionali nel quadro regolamentare nazionale e di allinearsi alle previsioni della Direttiva CRD IV, oltre che di procedere a una razionalizzazione del quadro normativo preesistente alla luce dei provvedimenti emanati in materia negli ultimi anni, ha condotto la Banca d'Italia all'emanazione di nuove disposizioni che mirano a rafforzare la capacità delle banche di gestire i rischi e di promuovere la sana e prudente gestione. Le *Disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni, sistema informativo e continuità operativa*, di seguito, per semplicità, Disposizioni, sono entrate in vigore il 3 luglio 2013, in seguito alla pubblicazione del 15° aggiornamento del 2 luglio 2013 alla Circolare 263/2006. Con il suddetto aggiornamento sono inseriti nel Titolo V della Circolare 263/2006 il Capitolo 7 "Il sistema dei controlli interni", il Capitolo 8 "Il sistema informativo" e il Capitolo 9 "La continuità operativa".
La Banca d'Italia, molto prima di procedere con l'emanazione del 15° aggiornamento e precisamente il 4 settembre 2012, ha reso pubblico il documento per la consultazione della proposta di disciplina.
La procedura di consultazione, come di consueto, ha permesso a chiunque di trasmettere, entro 60 giorni dalla pubblicazione, all'indirizzo p.e.c. della Banca d'Italia o tramite posta cartacea, le osservazioni e i commenti relativi alla proposta di disciplina.
A consultazione conclusa, la Banca d'Italia ha pubblicato, secondo le regole della consultazione pubblica, i commenti avanzati da parte dei partecipanti alla consultazione, un resoconto delle osservazioni ricevute, la relazione sull'analisi d'impatto della regolamentazione (AIR – Analysis Impact Regulatory) e il testo definitivo delle Disposizioni.

Il 16 dicembre 2013 la Banca d'Italia ha pubblicato un ulteriore documento per la consultazione pubblica contenente modifiche alle disposizioni in materia di organizzazione e governo societario emanate nel marzo 2008, fissando la scadenza per osservazioni e commenti al 14 gennaio 2014, data successivamente prorogata al 23 gennaio 2014.
Le nuove norme danno attuazione alla direttiva CRD IV per le parti relative agli assetti di governo societario delle banche, e tengono conto delle Linee guida emanate dall'EBA nel settembre 2011 sulla governance interna.
Le nuove disposizioni di vigilanza sul governo societario delle banche sono state emanate, ad esito dell'analisi delle osservazioni pervenute durante la consultazione pubblica, il 6 maggio 2014 e rappresentano il 1° aggiornamento alla Circolare n. 285 del dicembre 2013. Sono, infatti, confluite nel Titolo IV, Capitolo 1, della suddetta Circolare.

Ai fini della nostra analisi affronteremo nei paragrafi successivi e nel Capitolo 2 le Disposizioni in materia di sistema dei controlli interni contenute nel Capitolo 7, Titolo V, Circolare 263/2006,

tralasciando le disposizioni contenute nei due capitoli successivi. Dedicheremo, altresì, l'ultimo paragrafo del presente capitolo al 1° aggiornamento alla Circolare 285/2013.

1.2 Lo schema della nuova disciplina sui controlli interni: le finalità e i principi di fondo

Il Capitolo 7, inserito nel Titolo V della Circolare 263/2006, definisce un quadro organico di principi e regole cui deve essere ispirato il sistema dei controlli interni, aventi l'obiettivo di perseguire le finalità riportate all'interno del Box 1. La nuova disciplina non esaurisce, tuttavia, le disposizioni applicabili alle banche, rappresentando, infatti, la cornice di riferimento nella quale si inquadrano le regole sui controlli dettate all'interno di specifici ambiti disciplinari, che ne completano e integrano la portata (c.d. modello "hub and spokes")[21].

Box 1 - *Le finalità delle Disposizioni*

Le principali finalità della nuova disciplina sono:

- il rafforzamento della capacità delle banche di gestire i rischi aziendali, in linea con l'esperienza della recente crisi finanziaria che ha messo in luce il ruolo centrale della governance e del sistema dei controlli interni per assicurare la sana e prudente gestione delle banche e la stabilità del sistema finanziario;
- la revisione organica del vigente quadro normativo, resasi necessaria a seguito dell'emanazione, negli ultimi anni, di una serie di disposizioni, non solo di vigilanza, linee guida e raccomandazioni, che hanno interessato il funzionamento del sistema dei controlli interni, alcune delle quali già rammentate nel paragrafo precedente; tra tutte, rileva l'esigenza di allineamento alle previsioni contenute nella Direttiva CRD IV;
- la definizione di un quadro normativo omogeneo che, in base al principio di proporzionalità, tiene conto della natura dell'attività svolta, della tipologia dei servizi prestati, della complessità e della dimensione operativa delle banche[22].

In questo ambito, le disposizioni contenute nel Capitolo 7 definiscono:

- i principi generali del sistema dei controlli interni (Capitolo 7, Sezione I);
- il ruolo degli organi aziendali, a cui è rimessa la responsabilità primaria di formalizzare le politiche di governo dei rischi, di istituire il processo di gestione dei rischi e di procedere al loro riesame periodico (Capitolo 7, Sezione II);
- l'istituzione e i compiti delle funzioni aziendali di controllo (Capitolo 7, Sezione III);
- una disciplina organica in materia di esternalizzazione di funzioni aziendali al di fuori del gruppo bancario (Capitolo 7, Sezione IV);
- il Risk Appetite Framework, il sistema dei controlli interni e l'esternalizzazione nei gruppi bancari (Capitolo 7, Sezione V);
- le imprese di riferimento (Capitolo 7, Sezione VI);
- le regole applicabili alle succursali di banche comunitarie e di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci o in quelli inclusi nell'elenco pubblicato dalla Banca d'Italia (Capitolo 7, Sezione VII);
- l'informativa alla Banca d'Italia (Capitolo 7, Sezione VIII);
- le linee guida in materia di controlli interni relativamente a specifiche categorie di rischio (Capitolo 7, Allegato A);
- i controlli sulle succursali estere (Capitolo 7, Allegato B);
- le finalità e il contenuto minimale del Risk Appetite Framework (Capitolo 7, Allegato C).

[21] Cfr. Banca d'Italia, *Documento per la consultazione. Disposizioni di vigilanza prudenziale per le banche. Sistema dei controlli interni, sistema informativo e continuità operativa*, Relazione Illustrativa, 4 settembre 2012.
[22] *Ibid.*

La nuova disciplina si ispira ad alcuni principi di fondo messi in evidenza all'interno del Box 2 e, fatte salve alcune eccezioni, sarà efficace a partire dal 1° luglio 2014.

Box 2 - *I principi di fondo delle Disposizioni*

Le previsioni contenute all'interno del Capitolo 7 si ispirano ai seguenti principi di fondo:

- la valorizzazione del principio di proporzionalità, secondo cui le banche applicano le disposizioni tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati (cfr. Capitolo 7, Sezione I, par. 1);
- l'adozione di un approccio integrato alla gestione dei rischi o visione integrata dei rischi, che si traduce non solo nella diffusione di un linguaggio comune nella gestione dei rischi a tutti i livelli della banca e nell'adozione di metodi e strumenti di rilevazione e valutazione tra di loro coerenti (cfr. Capitolo 7, Sezione I, par. 6), ma anche nella possibilità di prevedere un piano di rotazione delle risorse tra le funzioni aziendali di controllo (cfr. Capitolo 7, Sezione III, par. 1);
- la diffusione di una cultura dei controlli interni attraverso: il rilievo strategico nella scala dei valori aziendali e il ruolo centrale nell'organizzazione aziendale attribuiti al sistema dei controlli interni, che deve coinvolgere organi, strutture, livelli gerarchici e personale nello sviluppo e nell'applicazione di metodi per identificare, misurare, comunicare e gestire i rischi (Capitolo 7, Sezione I, par. 6); l'approvazione, da parte dell'organo con funzione di supervisione strategica, di un codice etico, contenete i principi di condotta a cui deve essere improntata l'attività aziendale, cui sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti (cfr. Capitolo 7, Sezione II, par. 2); lo sviluppo e l'attuazione, da parte dell'organo con funzione di gestione, di programmi di formazione per sensibilizzare i dipendenti in merito alle responsabilità in materia di rischi, agevolando lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata (cfr. Capitolo 7, Sezione II, par. 3);
- il crescente coinvolgimento degli organi di vertice (l'organo con funzione di supervisione strategica, l'organo con funzione di gestione e l'organo con funzione di controllo) sui quali ricade, ciascuno secondo le rispettive competenze, la responsabilità primaria della definizione di un sistema dei controlli interni completo, adeguato, funzionale e affidabile (cfr. Capitolo 7, Sezione I, par. 1; Capitolo 7, Sezione II, par. 1 e seguenti);
- l'attenzione ai temi dell'efficienza e dell'efficacia dei controlli (cfr. Capitolo 7, Sezione I, par. 1; Capitolo 7, Sezione II, par. 1) e del coordinamento dei controlli (cfr. Capitolo 7, Sezione II, par. 5), assicurabile attraverso l'approvazione da parte dell'organo con funzione di supervisione strategica di uno specifico documento in cui devono essere definiti compiti, responsabilità e modalità di coordinamento/collaborazione tra le funzioni aziendali di controllo (Compliance, Risk management e Internal audit) e gli organi aziendali con compiti di controllo[23].

[23] Cfr. Marangoni M., *Il provvedimento di Banca d'Italia sul sistema dei controlli interni, impatti e novità*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

1.3 Il nuovo sistema dei controlli interni: principi generali

Le previsioni di cui alla Sezione I del Capitolo 7, rubricata "Disposizioni preliminari e principi generali", introducono i principi generali cui il sistema dei controlli interni si deve uniformare.

1.3.1 La definizione e i compiti del sistema dei controlli interni

L'Autorità di vigilanza, in premessa alla Sezione I del Capitolo 7, declina il sistema dei controlli interni come "un elemento fondamentale del complessivo sistema di governo delle banche; esso assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali e sia improntata a canoni di sana e prudente gestione"[24].
Viene, inoltre, adottata una nuova definizione di sistema dei controlli interni, riportata all'interno del Box 3, che testimonia la rilevanza che il sistema dei controlli interni deve assumere nell'ambito del governo delle banche, essendo finalizzato, tra l'altro, ad assicurare che l'attività sia in linea con le strategie e le politiche aziendali e sia improntata alla sana e prudente gestione, ad assicurare il contenimento del rischio entro il limite massimo accertato e a verificare il rispetto della conformità delle operazioni, non solo con la normativa di vigilanza, ma anche con le norme contenute nel Progetto di Governo Societario, nel Regolamento delle funzioni di controllo e in ogni altra disposizione interna[25].

Box 3 - *La definizione di sistema dei controlli interni*

Le Disposizioni identificano il sistema dei controlli interni nell'insieme "delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

- verifica dell'attuazione delle strategie e delle politiche aziendali;
- contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca (Risk Appetite Framework – "RAF") (cfr. Allegato C.);
- salvaguardia del valore delle attività e protezione delle perdite;
- efficacia e efficienza dei processi aziendali;
- affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;
- prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite [...];
- conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne"[26].

Tra i principi generali richiamati nella Sezione I possiamo senza dubbio inserire i seguenti (cfr. Capitolo 7, Sezione I, par. 1):

- i presidi relativi al sistema dei controlli interni devono coprire ogni tipo di rischio aziendale;
- la responsabilità primaria è rimessa agli organi aziendali, ciascuno secondo le proprie competenze;
- l'articolazione dei compiti e delle responsabilità degli organi e delle funzioni deve essere chiaramente definita.

[24] Banca d'Italia, *Circ. n. 263 del 27/12/2006, op.* cit., Titolo V, Capitolo 7, Sezione I, par. 1.
[25] Cfr. Priori M., Guglielmetti R., *Gli assetti di governo e controllo delle banche: la circolare di Banca d'Italia*, in Osservatorio di diritto bancario del Sole 24 ORE, 11 ottobre 2013.
[26] Banca d'Italia, *Circ. n. 263 del 27/12/2006, op. cit.*, Titolo V, Capitolo 7, Sezione I, par. 6.

La realizzazione delle finalità assegnate al sistema dei controlli interni richiede che a quest'ultimo debbano essere assegnati alcuni compiti generali come mostrato all'interno del Box 4.

Box 4 - *I compiti del sistema dei controlli interni*

Il sistema dei controlli interni deve "in generale:

- assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia), l'affidabilità del processo di gestione dei rischi e la sua coerenza con il RAF;
- prevedere attività di controllo diffuse a ogni segmento operativo e livello gerarchico;
- garantire che le anomalie siano tempestivamente portate a conoscenza di livelli appropriati dell'impresa (agli organi aziendali, se significative) in grado di attivare tempestivamente gli opportuni interventi correttivi;
- incorporare specifiche procedure per far fronte all'eventuale violazione di limiti operativi"[27].

Vengono inoltre stabilite e richiamate più volte dalle Disposizioni le caratteristiche di base del sistema dei controlli interni che si riferiscono ai concetti di completezza, adeguatezza, funzionalità e affidabilità dello stesso (cfr. ad es. Capitolo 7, Sezione I, par. 1; Capitolo 7, Sezione I, par. 6; Capitolo 7, Sezione II, par. 1; Capitolo 7, Sezione II, par. 4; ecc.).

In linea, peraltro, con quanto affermato dai più recenti orientamenti in materia, al sistema dei controlli interni viene attribuito dalla Vigilanza un ruolo centrale nell'organizzazione aziendale. Esso, infatti, rappresenta un elemento fondamentale di conoscenza per gli organi aziendali tale da garantire piena consapevolezza della situazione ed efficace presidio dei rischi aziendali e delle loro interrelazioni[28], orienta i mutamenti delle linee strategiche e delle politiche aziendali e adatta in modo coerente il contesto organizzativo, presidia la funzionalità dei sistemi gestionali e il rispetto degli istituti di vigilanza prudenziale e favorisce la diffusione di una corretta cultura dei rischi, della legalità e dei valori aziendali (cfr. Capitolo 7, Sezione I, par. 6).

Ciò posto, il sistema dei controlli interni ha e deve avere rilievo strategico nell'implementazione dell'attività bancaria, e la cultura del controllo, principio di fondo della nuova disciplina, deve assumere una posizione di rilievo strategico nella scala dei valori aziendali: "non riguarda solo le funzioni aziendali di controllo, ma coinvolge tutta l'organizzazione aziendale (organi aziendali, strutture, livelli gerarchici, personale), nello sviluppo e nell'applicazione di metodi, logici e sistematici, per identificare, misurare, comunicare, gestire i rischi"[29].

1.3.2 Il processo di gestione dei rischi e i principi generali di organizzazione

Con riferimento alle tipologie di controllo e alla conseguente strutturazione organizzativa delle funzioni aziendali ad esso dedicate, viene ribadita e confermata, ma meglio esplicitata, la ripartizione tra controlli di linea o di primo livello, controlli sui rischi e sulla conformità o di secondo livello e revisione interna o controlli di terzo livello[30]. Le Disposizioni precisano che i controlli di 2° livello devono essere affidati a funzioni distinte da quelle produttive, che sono coinvolte nella definizione delle politiche di governo dei rischi e del processo di gestione dei rischi (cfr. Capitolo 7, Sezione I, par. 6).

[27] *Ibid*.
[28] Cfr. Priori M., Guglielmetti R., *Gli assetti di governo e controllo delle banche: la circolare di Banca d'Italia*, op. cit.
[29] Banca d'Italia, *Circ. n. 263 del 27/12/2006,* op. cit., Titolo V, Capitolo 7, Sezione I, par. 6.
[30] Per approfondimenti si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 6.

Rispetto al previgente quadro normativo sono declinati specifici principi generali di organizzazione, segnalati all'interno del Box 5, che, oltre agli aspetti strettamente pertinenti al sistema dei controlli, riguardano altri profili, quali ad esempio le politiche di gestione delle risorse umane e la prevenzione dei conflitti di interesse.
Particolare attenzione merita il principio relativo ai processi e alle metodologie di valutazione. L'obbligo per le banche di definire processi e metodologie di valutazione, anche a fini contabili, delle attività aziendali in modo integrato con il processo di gestione del rischio, risulta essere, infatti, una delle novità di rilievo rispetto al previgente quadro normativo, che affronteremo nel capitolo seguente.

Box 5 - *I principi generali di organizzazione*

Le attuali Disposizioni prevedono che le banche devono rispettare i seguenti principi generali di organizzazione (cfr. Capitolo 7, Sezione I, par. 6):

- i processi decisionali e l'affidamento di funzioni al personale sono formalizzati e consentono l'univoca individuazione di compiti e responsabilità e sono idonei a prevenire i conflitti di interessi. In tale ambito, deve essere assicurata la necessaria separatezza tra le funzioni operative e quelle di controllo;
- le politiche e le procedure di gestione delle risorse umane assicurano che il personale sia provvisto delle competenze e della professionalità necessarie per l'esercizio delle responsabilità a esso attribuite;
- il processo di gestione dei rischi è efficacemente integrato. Sono considerati parametri di integrazione, riportati a titolo esemplificativo e non esaustivo: la diffusione di un linguaggio comune nella gestione dei rischi a tutti i livelli della banca; l'adozione di metodi e strumenti di rilevazione e valutazione tra di loro coerenti (ad es., un'unica tassonomia dei processi e un'unica mappa dei rischi); la definizione di modelli di reportistica dei rischi; l'individuazione di momenti formalizzati di coordinamento ai fini della pianificazione delle rispettive attività; la previsione di flussi informativi su base continuativa tra le diverse funzioni in relazione ai risultati delle attività di controllo di propria pertinenza; la condivisione nella individuazione delle azioni di rimedio;
- i processi e le metodologie di valutazione, anche a fini contabili, delle attività aziendali sono affidabili e integrati con il processo di gestione del rischio. A tal fine: la definizione e la convalida delle metodologie di valutazione sono affidate a unità differenti; le metodologie di valutazione sono robuste, testate sotto scenari di stress e non fanno affidamento eccessivo su un'unica fonte informativa; la valutazione di uno strumento finanziario è affidata a un'unità indipendente rispetto a quella che negozia detto strumento;
- le procedure operative e di controllo devono: minimizzare i rischi legati a frodi o infedeltà dei dipendenti; prevenire o, laddove non sia possibile, attenuare i potenziali conflitti d'interesse; prevenire il coinvolgimento, anche inconsapevole, in fatti di riciclaggio, usura o di finanziamento al terrorismo;
- il sistema informativo rispetta la disciplina del Capitolo 8 (Il sistema informativo);
- i livelli di continuità operativa garantiti sono adeguati e conformi a quanto stabilito dal Capitolo 9 (La continuità operativa).

1.4 Le nuove disposizioni sulla governance

Come anticipato all'interno del primo paragrafo del presente capitolo, con il 1° aggiornamento del 6 maggio 2014 alla Circolare 285/2013, la Banca d'Italia ha inserito nella prima parte della citata Circolare il Titolo IV, rubricato "Governo societario, controlli interni, gestione dei rischi", nel quale sono confluite le nuove disposizioni in materia di organizzazione e governo societario. Con la loro entrata in vigore sono state abrogate le precedenti disposizioni di vigilanza in materia di organizzazione e governo societario delle banche del 4 marzo 2008.

Con l'aggiornamento in oggetto la Banca d'Italia ha inteso dare attuazione alle disposizioni contenuta nella CRD IV in materia di governo societario, tenendo conto, anche, degli orientamenti sull'organizzazione interna emanati dall'EBA nel settembre 2011[31].
La CRD IV prevede, infatti, una disciplina in materia di governo societario più organica e puntuale rispetto ai soli principi generali di cui all'abrogato art. 22 della CRD. Il suo recepimento ha, quindi, reso necessario operare alcune integrazioni della normativa nazionale soprattutto in materia di:

- istituzione, composizione e funzioni dei comitati interni al C.d.a.;
- coinvolgimento dei singoli Consiglieri, per assicurare che ognuno agisca con indipendenza e dedichi sufficiente tempo all'incarico;
- piani di formazione dei soggetti che ricoprono ruoli chiave all'interno della banca;
- informativa da rendersi al pubblico sul sito web.

Con riferimento, invece, alle *Linee Guida* emanate dall'EBA, è necessario precisare che alcune di esse erano già state recepite con la *Comunicazione* del gennaio 2012[32], mentre altre, in materia di composizione quantitativa degli organi, numero adeguato dei componenti, piani di successione, ruolo del presidente e processo di autovalutazione, costituiscono oggetto di alcune delle novità introdotte dalla nuova disciplina, la cui importanza è emersa anche in sede applicativa.

Inoltre, il recepimento della CRD IV ha rappresentato l'occasione per incorporare nel testo delle disposizioni i chiarimenti e gli indirizzi già forniti al sistema con la *Nota di chiarimenti* del febbraio 2009 e la *Comunicazione* del 2012, e coordinare le stesse disposizioni con gli altri provvedimenti emanati di recente dalla Banca d'Italia, come la nuova disciplina in materia di sistema dei controlli interni, e con il prossimo avvio del Single Supervisory Mechanism. Con riferimento a questo ultimo punto, è stato rivisto il criterio di proporzionalità già presente nella normativa attuale per assicurare che nell'insieme delle "banche di maggiori dimensioni e complessità operativa" vi ricadano tutte quelle considerate "significative" ai sensi del Regolamento sul Sistema di Supervisione Unico Europeo.

Infine, il testo delle nuove disposizioni contiene precisazioni e chiarimenti opportuni alla luce dell'esperienza applicativa maturata sulle modalità di applicazione corretta delle norme. I punti interessati riguardano, in particolare, il principio di non pletoricità degli organi, le banche popolari, il processo di autovalutazione del Consiglio e il ruolo del Presidente.

[31] EBA, *Guidelines on Internal Governance*, op. cit.

[32] Banca d'Italia, *Applicazione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, op. cit. Si fa riferimento, in particolare, ai principi in tema di comitato per il controllo interno rischi, funzionamento del C.d.a. e processo di nomina, e si rinvia, alla citata *Comunicazione* del 2012.

CAPITOLO 2

Le principali novità rispetto al previgente quadro normativo in materia di sistema dei controlli interni

Le disposizioni in materia di sistema dei controlli interni, contenute nel Capitolo 7, introducono alcune novità di rilievo rispetto al previgente quadro normativo, al fine di dotare le banche di un sistema dei controlli interni completo, adeguato, funzionale e affidabile.

L'Autorità di vigilanza ha operato un'analisi costi-benefici di alcuni degli aspetti innovativi della nuova normativa per i quali erano state individuate diverse opzioni regolamentari.
Su questo si soffermano, dapprima, la relazione preliminare sull'analisi d'impatto della regolamentazione (AIR - Analysis Impact Regulatory) e poi quella definitiva (di seguito, rispettivamente, AIR preliminare e AIR definitiva), che beneficia dei contributi giunti nel corso della consultazione.
L'AIR definitiva evidenzia come, nel complesso i benefici delle innovazioni regolamentari superebbero i costi stimati, considerato che un più robusto sistema dei controlli interni contribuisce senz'altro alla sana e prudente gestione delle banche, e a una più efficace gestione dei rischi. Peraltro, interventi sul sistema dei controlli interni comportano anche costi, legati principalmente all'esigenza di dotare le funzioni di controllo di risorse più numerose e più qualificate, e di modificare procedure e processi aziendali. In generale, l'AIR definitiva segala che l'attuazione delle Disposizioni secondo le opzioni suggerite comporta costi d'impianto moderati e costi ricorrenti relativamente contenuti. A fronte di questo, le banche potranno beneficiare di un migliore allineamento del risk appetite con la gestione dei rischi, nonché di una maggiore efficienza della stessa. Sia la struttura sia il funzionamento in concreto degli organi incaricati dei controlli interni dovrebbero registrare benefici sul piano della completezza, efficienza ed efficacia. La maggiore solidità degli intermediari potrà contribuire a rendere il sistema più robusto nel suo complesso, con benefici anche per il sistema economico. L'AIR definitiva, nel trarre le conclusioni dell'analisi compiuta, afferma che la percezione di costi presumibilmente elevati da parte degli intermediari di minori dimensioni è stata attentamente valutata nella versione definitiva delle Disposizioni, soprattutto in un'ampia declinazione del principio di proporzionalità.

Ai fini della nostra analisi, il presente capitolo affronta le principali novità del nuovo framework dei controlli, suddividendole in due macroaree: le novità in tema di governance (par. 2.1) e gli elementi innovativi riferibili al controllo dei rischi (par. 2.2).

2.1 Le innovazioni in tema di governance

Con riferimento alla governance, a fronte dell'obiettivo generale di rafforzare la capacità delle banche di gestire i rischi e di promuovere la sana e prudente gestione, la nuova normativa innova principalmente nei seguenti aspetti:

- la valutazione delle attività aziendali;
- il ruolo degli organi aziendali;
- l'organismo di vigilanza ex d.lgs. 231/2001;
- il coordinamento di organi e funzioni di controllo.

2.1.1 La formalizzazione dei processi e delle metodologie di valutazione delle attività aziendali

Nella crisi finanziaria, al venir meno della liquidità sui mercati di strumenti complessi e all'indisponibilità di prezzi sui mercati secondari, le banche hanno sperimentato la necessità di passare da metodi di valutazione basati sui prezzi osservabili a valutazioni basate su metodi teorici, incontrando, tuttavia, difficoltà nell'affidarsi a metodologie robuste e in grado di prezzare il rischio intrinseco di prodotto complessi. La perdita di fiducia tra creditori,

controparti e clienti sulle pratiche di valutazione delle banche di certe attività finanziarie ha contribuito direttamente al ritiro di fondi e alla crisi di liquidità sui mercati. Alla luce di questo l'Autorità di vigilanza ha considerato una necessità imporre lo sviluppo di processi di valutazione robusti, efficaci e affidabili, soprattutto a tutela dell'operatività degli intermediari i cui portafogli presentano elevate percentuali di strumenti complessi[33].

Le banche sono, pertanto, obbligate a dotarsi e formalizzare processi e metodologie di valutazione delle attività affidabili e integrati con il processo di gestione del rischio. A tal fine devono essere rispettati i seguenti requisiti (cfr. Capitolo 7, Sezione I, par. 6):

i. il processo di valutazione delle attività deve articolarsi in due unità differenti per la definizione e la validazione delle metodologie di valutazione;
ii. le metodologie di valutazione devono essere testate sotto scenari di stress e non devono fare affidamento eccessivo su un'unica fonte informativa;
iii. la valutazione di uno strumento finanziario deve essere affidata a un'unità indipendente rispetto a quella responsabile della negoziazione.

L'AIR definitiva, pubblicata dalla Banca d'Italia nel giugno 2013, evidenzia i benefici e i costi dell'opzione regolamentare adottata (anche le disposizioni poste in consultazione incorporavano la stessa opzione), che si contrapponeva all'ipotesi di mantenimento dello status quo (nessun obbligo di formalizzare il processo di valutazione).
A fronte di benefici che sembrerebbero elevati per tutti i soggetti interessati, i costi di compliance individuati, legati all'attuazione dell'opzione adottata, sarebbero sia una tantum (legati alla definizione del processo, all'individuazione dei ruoli, allo sviluppo di metodologie e alla valorizzazione di più fonti informative) sia ricorrenti, volti a verificare l'adeguatezza nel continuo del processo di valutazione. Come sperimentato nella crisi finanziaria, disporre di valutazioni robuste ed efficaci permette agli intermediari di gestire meglio e più consapevolmente i rischi insiti nei diversi strumenti finanziari, con una corrispondente maggiore possibilità di limitare le perdite, accrescendo la stabilità del sistema e registrando effetti positivi sull'economia nel suo complesso. D'altro canto, però, la formalizzazione del processo di valutazione e il suo funzionamento si possono tradurre in maggiori costi per il personale dovuti all'esigenza di accrescere qualitativamente e quantitativamente le risorse allocate alla funzione. Tali costi, tuttavia, precisa l'AIR definitiva, sarebbero nel complesso limitati ai soli oneri incrementali rispetto al mantenimento di procedure già esistenti a tali fini. Per quanto concerne le altre tipologie di costo, l'AIR non ravvisa significativi costi diretti o di controllo per l'Autorità di vigilanza, né costi indiretti per gli altri portatori di interessi.
L'AIR definitiva evidenzia, inoltre, quanto emerso nell'ambito della procedura di consultazione in merito alla valutazione dei costi derivanti dall'opzione adottata.
La Banca d'Italia, infatti, nella sua AIR preliminare, invitava, gli intermediari a rispondere ad alcuni quesiti concernenti il processo di valutazione delle attività aziendali implementato al loro interno, con particolare riferimento alle caratteristiche dello stesso, alla presenza di stress test applicati alle metodologie di valutazione adottate, ai costi da sostenere per la formalizzazione del processo di valutazione secondo le caratteristiche definite dalla normativa.
L'AIR definitiva segnala che, in merito ai costi che tale processo di valutazione comporterebbe, è emersa la diversa situazione in cui incorrerebbero gli intermediari minori rispetto a quelli di maggiore dimensione. Mentre gli ultimi qualificano i costi addizionali come poco più elevati, per i primi i costi di attuazione del processo sarebbero molto elevati. Questo ha spinto gli intermediari minori a richiedere gradualità e flessibilità per consentire la definizione e l'attuazione di soluzioni di sistema per la categoria.

[33] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.

2.1.2 Il ruolo degli organi aziendali: nuovi compiti e nuove responsabilità

Le Disposizioni enfatizzano il ruolo degli organi aziendali, primi responsabili, ciascuno per le proprie competenze, della definizione di un sistema dei controlli interni completo, adeguato, funzionale e affidabile, nonché della formalizzazione del quadro di riferimento per la determinazione della propensione al rischio (Risk Appetite Framework – RAF), delle politiche di governo e del processo di gestione dei rischi. In merito, le Disposizioni forniscono "indicazioni minime circa il ruolo di ciascun organo aziendale nell'ambito del sistema dei controlli interni, anche al fine di chiarirne i relativi compiti e responsabilità"[34]. L'esigenza di cambiamento finalizzata a un presidio effettivo dei rischi è stata quindi soddisfatta anche mediante un'assegnazione puntuale del ruolo di ciascuno organo nella definizione ex ante e nella gestione in itinere di livelli di rischio adeguati e sostenibili, in linea con gli indirizzi di programmazione strategica adottati dalla banca[35].

Come chiaramente indicato dalle Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche, emanate dalla Banca d'Italia nel marzo 2008 e di recente modificate, i compiti e poteri di amministrazione e di controllo devono essere ripartiti in modo chiaro ed equilibrato tra i diversi organi, evitando concentrazioni di potere che possano impedire una corretta dialettica interna.
Si tratta del c.d. bilanciamento dei poteri, principio base di un sistema di governo efficiente e obiettivo generale perseguito dalle disposizioni in materia di organizzazione e governo societario. In particolare, quando le funzioni di supervisione strategica e di gestione sono incardinate in un solo organo, viene richiesto un equilibrato bilanciamento dei poteri tra i componenti non esecutivi e quelli esecutivi dell'organo stesso. Tale distinzione di potere consente una più puntuale articolazione dei momenti (di supervisione e gestionali) attraverso i quali l'organo medesimo esercita le proprie competenze[36].
Questo principio viene puntualizzato per la prima volta in maniera dettagliata dalla nuova normativa sui controlli interni. Infatti, il Capitolo 7 della Circolare 263/2006 dedica la Sezione II al ruolo degli organi aziendali, fornendo indicazioni circa il ruolo di ciascun organo aziendale, al fine di chiarirne i relativi compiti e responsabilità.

Di particolare evidenza risultano i compiti in materia di controlli interni attribuiti dalla nuova normativa all'organo con funzione di supervisione strategica, coincidente, nel sistema tradizionale, con il Consiglio di amministrazione (C.d.a.).
Con l'espressione "organo con funzione di supervisione strategica", le nuove Disposizioni si riferiscono a: "l'organo aziendale a cui […] sono attribuite funzioni di indirizzo della gestione dell'impresa, mediante, tra l'altro, esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche"[37].
L'organo in questione svolge un ruolo centrale nel sistema di governo, essendo chiamato, tra l'altro, a deliberare sugli indirizzi di carattere strategico della banca e a verificarne l'attuazione[38]. Per tale ragione, la Banca d'Italia, dopo aver chiarito nel 2008, mediante la fissazione di principi generali e linee guida successivamente modificati, l'importanza di tale organo in termini di autorevolezza, professionalità e composizione diversificata, con il 15° aggiornamento alla Circolare 263/2006, è ulteriormente intervenuta sul punto, delineando una

[34] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione II, par. 1.
[35] Cfr. Priori M., Guglielmetti R., *Sistema dei controlli interni: l'organo con funzione di supervisione strategica*, in Osservatorio di diritto bancario del Sole 24 ORE, 23 ottobre 2013.
[36] Cfr. Sottoriva C., *Collegio sindacale e sistema dei controlli interni nell'ambito delle aziende di credito alla luce delle nuove disposizioni di vigilanza prudenziale (Banca d'Italia 2 luglio 2013) e della Direttiva 2013/36/UE*, in Rivista di Diritto Bancario, n. 12/2013.
[37] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 3.
[38] Per un completo approfondimento dei compiti assegnati all'organo con funzione di supervisione strategica si fa rinvio a Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione II, par. 2.

cornice piuttosto definita dei compiti del C.d.a., ben differenziandoli da quanto, invece, di competenza dell'organo con funzioni di gestione[39].
In particolare, le nuove norme enfatizzano il ruolo di questo organo, attribuendogli, tra gli altri, i nuovi compiti riportati all'interno del Box 6.

Box 6 - *I nuovi compiti dell'organo con funzione di supervisione strategica*

Le Disposizioni assegnano all'organo con funzione di supervisione strategica il compito di:

- definire il livello di rischio tollerato (c.d. tolleranza al rischio o appetito per il rischio) (cfr. Capitolo 7, Sezione II, par. 2);
- definire i criteri per l'individuazione delle operazioni di maggiore rilevanza (cfr. Capitolo 7, Sezione II, par. 2);
- approvare le politiche e i processi di valutazione delle attività, in particolare degli strumenti finanziari, e stabilire i limiti massimi all'esposizione verso strumenti o prodotti finanziari di incerta o difficile valutazione (cfr. Capitolo 7, Sezione II, par. 2);
- definire, insieme all'organo con funzione di gestione che ne cura anche l'attuazione, il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività e l'inserimento in nuovi mercati (cfr. Capitolo 7, Sezione II, parr. 2 e 3).
- definire la politica in materia di esternalizzazione di funzioni aziendali (cfr. Capitolo 7, Sezione II, par. 2);
- favorire la diffusione di una cultura dei controlli attraverso l'approvazione di un codice etico al quale sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti (cfr. Capitolo 7, Sezione II, par. 2);
- approvare il piano pluriennale di audit (cfr. Capitolo 7, Sezione II, par. 2)[40].

Tali novità richiederanno alle banche di verificare che i compiti e i poteri del C.d.a. prevedano l'adempimento dei nuovi compiti attribuiti all'organo amministrativo, e di integrare, dove necessario, la regolamentazione interna con i nuovi adempimenti.

Le previsioni in materia di organi aziendali, a cui è dedicata l'intera Sezione II, introducono alcune novità anche con riferimento ai compiti e alle responsabilità dell'organo con funzione di gestione, a cui partecipa tipicamente il Direttore generale (D.g.), figura a capo dell'Alta direzione (A.d.).
La nuova normativa in materia di sistema dei controlli interni specifica che con l'espressione "organo con funzione di gestione" si intende: " l'organo aziendale o i componenti di esso a cui […] spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione"[41].
L'organo in questione, è, quindi, l'organo aziendale (ad esempio, il comitato esecutivo) o il/i soggetto/i (ad esempio, l'amministratore delegato o gli amministratori delegati) ai quali spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati dal

[39] Cfr. Priori M., Guglielmetti R., *Sistema dei controlli interni: l'organo con funzione di supervisione strategica*, op. cit.
[40] Cfr. Fumagalli M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.
[41] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 3.

C.d.a.[42]. In tale definizione è inclusa anche la figura del D.g., figura che, però, non può essere identificata con l'organo con funzione di gestione[43].
In particolare, le nuove norme enfatizzano il ruolo di questo organo, attribuendogli i nuovi compiti mostrati all'interno del Box 7.

Box 7 - *I nuovi compiti dell'organo con funzione di gestione*

Le previsioni dedicate all'organo con funzione di gestione assegnano a quest'ultimo il compito di (cfr. Capitolo 7, Sezione II, par. 3):

- nell'ambito dell'attuazione del processo di gestione dei rischi, stabilire i limiti operativi all'assunzione delle varie tipologie di rischio, coerentemente con la propensione al rischio e tenendo esplicitamente conto dei risultati delle prove di stress e dell'evoluzione del quadro economico; definire i programmi di formazione per sensibilizzare i dipendenti in merito alle responsabilità in materia di rischi; stabilire le responsabilità delle strutture e delle funzioni coinvolte nella gestione dei rischi, in modo che siano chiaramente definiti i relativi compiti e siano prevenuti potenziali conflitti di interesse; esaminare ed eventualmente autorizzare le operazioni di maggior rilevo oggetto di parere negativo da parte del risk management;
- definire e curare l'attuazione del processo (responsabili, procedure, condizioni) per approvare gli investimenti in nuovi prodotti, la distribuzione di nuovi prodotti/servizi ovvero l'avvio di nuove attività o l'ingresso in nuovi mercati;
- definire e curare l'attuazione della politica in materia di esternalizzazione di funzioni aziendali;
- definire e curare l'attuazione e l'aggiornamento dei processi e delle metodologie di valutazione delle attività aziendali approvate dal C.d.a., e, in particolare, degli strumenti finanziari;
- autorizzare il superamento della propensione al rischio entro il limite rappresentato dalla soglia di tolleranza, dandone pronta informativa all'organo con funzione di supervisione strategica, e individuare le azioni gestionali volte a ricondurre il rischio assunto entro l'obiettivo prefissato[44].

Anche tali novità richiederanno alle banche di verificare che tra i compiti e i poteri dell'organo con funzione di gestione vi siano anche quelli introdotti dalle Disposizioni, e di integrare, dove necessario, la regolamentazione interna con i nuovi adempimenti.

La nuova normativa in materia di sistema dei controlli interni fornisce minori indicazioni circa il ruolo, i compiti e le responsabilità dell'organo con funzione di controllo, che si identifica, nel sistema tradizionale, con il Collegio sindacale.
Con riferimento alla necessità di pervenire ad una revisione organica delle disposizioni in materia di sistema dei controlli interni, e in particolare all'opportunità di definire il ruolo dell'organo con funzione di controllo, le nuove Disposizioni rimandano, infatti, per la descrizione dettagliata dei compiti e dei poteri dell'organo in esame, alle disposizioni in materia di organizzazione del 2008 e successive modifiche.

[42] Per un completo approfondimento dei compiti assegnati all'organo con funzione di gestione si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione II, par. 3.
[43] Il divieto di identificazione nella figura del Direttore generale dell'organo con funzione di gestione, viene ribadito nell'ambito della *Nota di chiarimenti* pubblicata da Banca d'Italia il 24/01/2014 e aggiornata il 06/06/2014 attraverso la quale la stessa Autorità di vigilanza fornisce alcune indicazioni in merito all'applicazione della disciplina in materia di sistema dei controlli interni, sistema informativo e continuità operativa contenuta nei capitoli 7, 8 e 9 del Titolo V della Circ. 263/2006.
[44] Cfr. Fumagalli M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, op. cit.

Con l'espressione "organo con funzione di controllo", le nuove Disposizioni si riferiscono a: "il collegio sindacale, il consiglio di sorveglianza o il comitato per il controllo sulla gestione"[45].
Nel dettaglio, la nuova normativa dispone che: "l'organo con funzione di controllo ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni e del RAF. Nell'espletamento di tale compito, […] vigila sul rispetto delle previsioni di cui i) alla presente Sezione, ii) alla sezione I e III e iii) al processo ICAAP. Per lo svolgimento delle proprie attribuzioni, tale organo dispone di adeguati flussi informativi da parte degli altri organi aziendali e delle funzioni di controllo"[46].
In particolare, le nuove norme introducono, con riguardo alla figura dell'organo in esame, una sola novità di rilevo rispetto alla normativa di riferimento, concernente lo svolgimento delle funzioni affidate all'Organismo di vigilanza (O.d.V), eventualmente istituito ai sensi del d.lgs. 231/2001 in materia di responsabilità amministrativa degli enti. Tale novità verrà approfondita nel paragrafo successivo.

2.1.3 L'organismo di vigilanza ex d.lgs. 231/2001, il rapporto con l'organo con funzione di controllo e le osservazioni dell'Associazione dei Componenti degli Organismi di Vigilanza

L'assetto generale dei controlli interni è completato da un organismo la cui istituzione e il cui funzionamento sono disciplinati, come già accennato nel paragrafo precedente, dal d.lgs. 231/2001[47].
Il Decreto ha individuato un insieme di illeciti che, se commessi nell'interesse o a vantaggio dell'ente da parte di soggetti che rivestono funzioni di rappresentanza, amministrazione o direzione, o persone dirette o vigilate da queste, nonché illeciti commessi da persone che esercitano la gestione e il controllo dell'ente, comportano una responsabilità a carico dell'ente. Tale responsabilità è esclusa solo al ricorrere di talune condizioni, quali: l'adozione di modelli di organizzazione e gestione idonei alla prevenzione degli illeciti, l'affidamento del compito di vigilare sul funzionamento e sull'osservanza dei modelli a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo, detto Organismo di Vigilanza, di seguito anche O.d.V., nonché l'avvenuta elusione fraudolenta dei modelli stessi, e la non sufficiente vigilanza dell'organismo medesimo. La responsabilità degli enti per gli illeciti amministrativi dipendenti da reato viene così a dipendere in larga parte dal coretto ed efficace funzionamento dell'O.d.V. Pertanto, nonostante l'istituzione di un O.d.V. possa essere considerata una facoltà per l'ente, la sua presenza e il suo corretto funzionamento sembrano rappresentare un presidio fondamentale ai fini della prevenzione della commissione degli illeciti, oltre che uno dei presupposti per evitare l'automatica chiamata in corresponsabilità[48].

Stante la particolare delicatezza dell'interazione fra l'O.d.V. e l'organo con funzione di controllo, il nuovo comma 4bis dell'art. 6 del decreto citato, introdotto dall'art. 14 della Legge di stabilità 2012 (L. 183/2011), dispone che nelle società di capitali il Collegio sindacale, il Consiglio di sorveglianza e il Comitato per il controllo sulla gestione possono svolgere le funzioni dell'O.d.V. Il legislatore ha quindi permesso che i due organismi vengano a coincidere, dando la possibilità all'organo di controllo di accentrare su di sé lo svolgimento delle funzioni demandate all'O.d.V.
La nuova normativa stabilisce, invece, che l'organo con funzione di controllo svolge, di norma, le funzioni dell'organismo di vigilanza, e che le banche possono affidare tali funzioni a un organismo appositamente istituito previa adeguata motivazione (cfr. Capitolo 7, Sezione II, par.

[45] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 3.
[46] Ivi, Capitolo 7, Sezione I I, par. 4.
[47] D.Lgs. n. 231/2001, *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300.*
[48] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.

4). La disposizione in esame sembra, quindi, valorizzare il ruolo dell'organo con funzione di controllo, quale centrale presidio di legalità dell'attività sociale e organo apicale dell'intero sistema dei controlli.

La Banca d'Italia ha ricordato nell'aggiornamento del 06/06/2014 alla Nota di chiarimenti del 24/01/2014 che l'adeguatezza della motivazione va valutata alla luce dell'idoneità della particolare composizione prescelta per l'organismo ad assicurare il corretto espletamento dei compiti a esso attribuiti e un efficace coordinamento con il sistema dei controlli interni. Fermo restando l'autonomia della banca e le valutazioni della Vigilanza sui casi concreti, la Banca d'Italia sostiene che la presenza dei responsabili delle funzioni aziendali di controllo di 2° e 3° livello e del presidente dell'organo con funzione di controllo non appare incoerente con i principi della regolamentazione volti a favorire il coordinamento tra i vari soggetti preposti ai compiti di controllo e ad assicurare un adeguato grado di autonomia e indipendenza dell'organismo.

L'AIR definitiva, pubblicata dalla Banca d'Italia nel giugno 2013, evidenzia i benefici e i costi dell'opzione regolamentare adottata (l'AIR preliminare non affronta la novità in questione, se pur le disposizioni poste in consultazione già disponessero la coincidenza tra i due organi).
Le opzioni regolamentari disponibili erano le seguenti:

- HO: mantenimento dello status quo, ossia libera scelta sull'eventuale coincidenza dell'O.d.V. con l'organo con funzione di controllo;
- H1: coincidenza dei due organi, con possibilità di scelta difforme al ricorrere di particolari e motivate esigenze;
- H2: coincidenza dei due organi, con possibilità di scelta difforme al ricorrere di motivate esigenze.

Le Disposizioni hanno accolto, stante le riflessioni condotte alla luce dei risultati della consultazione, l'opzione indicata in H2, che rispetto all'opzione H1 prevede un ampliamento delle circostanze nelle quali la società può optare per la separatezza.
L'AIR definitiva, nei confronti della coincidenza dei due organi, individua i seguenti benefici:

- aumento dell'efficacia dei controlli, a motivo di un più efficiente flusso informativo, reso possibile dalla creazione di sinergie tra i due organi;
- accorciamento della catena dei controlli con conseguente riduzione dei costi dell'attività di controllo e recupero di efficienza.

A fronte di tali benefici, l'AIR evidenzia costi legati principalmente al fatto che le funzioni svolte dai due organi rispondono a finalità diverse. Da un lato, come noto, l'obiettivo perseguito dall'organo con funzione di controllo è evitare che si verifichino eventi pregiudizievoli per il corretto svolgimento dell'attività sociale. Dall'altro lato, invece, l'obiettivo è che i reati ex d.lgs. 231/2001 eventualmente commessi lo siano in violazione del modello di organizzazione e gestione predisposto. Inoltre, considerato che l'O.d.V. prevede la partecipazione di professionalità di natura diversa interne o esterne alla società, la coincidenza dei due organi potrebbe provocare la mancata valorizzazione delle differenze in termini di composizione fra l'organo con funzioni di controllo e l'O.d.V. Infine, la coincidenza potrebbe comportare una quasi automatica sottrazione dell'organo con funzione di controllo al controllo ex. d.lgs. 231/2001. Per quanto concerne le altre tipologie di costo non si ravvisano costi diretti per l'Autorità di vigilanza.
L'AIR segnala, inoltre, quanto criticato nell'ambito della procedura di consultazione in merito all'opzione adottata dalla proposta di normativa. I partecipanti alla consultazione hanno contestato l'obbligatorietà, essenzialmente in ogni caso, della coincidenza tra i due organi, a discapito della necessità di assicurare flessibilità organizzativa e riconoscere piena autonomia rispetto all'istituzione di un organo ad hoc o all'affidamento di tale ruolo all'organo con funzione di controllo. La coincidenza potrebbe, infatti, in alcune realtà, risultare inefficiente e

inefficace, potendo rivelarsi necessario delegare comunque alcune funzioni, con conseguente aggravio di costi.

Alcune osservazioni in merito alla disposizione in esame sono state formulate anche da parte dell'Associazione dei Componenti degli O.d.V. ex. d.lgs.231/2001 (AODV).
In primo luogo l'AODV paragona quanto disposto dalla Banca d'Italia e il comma 4bis dell'art. 6 del d.lgs. 231/2001.
Come già ricordato, tale norma, introdotta dalla Legge di Stabilità del 2012, permette all'organo con funzione di controllo di svolgere le funzioni dell'O.d.V.[49]. La Banca d'Italia, invece, nella disposizione in esame, si discosta dal legislatore del 2011, indicando come soluzione preferibile la coincidenza tra i due organi, indipendentemente dalle dimensioni e dalla complessità della realtà societaria, e considerando residuale e da motivare ogni altra soluzione. La conseguenza dell'applicazione di tale disposizione rischia dunque di essere che le banche si trovino a disporre di presidi preventivi subottimali rispetto alle prescrizioni del d.lgs. 231/2001, con ridotta capacità esimente della responsabilità amministrativa prevista dalle norme contenute nel decreto.
Inoltre, l'AODV fa notare che la Banca d'Italia, nel disporre l'attribuzione della funzione di O.d.V. all'organo di controllo, sembra prescindere dal dibattito inerente la formulazione originaria del comma 4bis dell'art.6, contenuta nella bozza della norma circolata nell'ottobre 2011. La bozza disponeva che nelle società di capitali l'organo con funzione di controllo avrebbe dovuto svolgere le funzioni dell'O.d.V. Tale proposta suscitò reazioni negative, a conferma delle convinzioni di dottrina e giurisprudenza, che, in passato, avevano osteggiato la totale coincidenza tra i due organi.
Per concludere, l'AODV afferma che non si ravvisano ragioni per cui alle banche venga imposta una soluzione organizzativa che la legge prevede invece, in ottica semplificatrice, come una mera facoltà per le società di capitali dotate di strutture di minore complessità.
Considerato che le osservazioni mosse dall'AODV sono riferibili al documento di consultazione delle nuove disposizioni in materia di sistema di controlli interni, la stessa associazione auspicava che la disposizione in esame fosse armonizzata con il disposto del sopracitato comma dell'art. 6. Come noto, le critiche avanzate non sono state accolte, dato che la formulazione del testo definitivo prevede l'attribuzione automatica del ruolo dell'O.d.V. all'organo con funzione di controllo.

2.1.4 Il documento di coordinamento di organi e funzioni di controllo

L'Autorità di vigilanza, dopo aver definito il ruolo e i compiti degli organi aziendali, si sofferma sulla necessità di garantire la "proficua interazione nell'esercizio dei compiti […] fra gli organi aziendali, gli eventuali comitati costituiti all'interno di questi ultimi, i soggetti incaricati della revisione legale dei conti, le funzioni di controllo"[50].

Le Disposizioni fanno riferimento, in particolare, alla proliferazione, all'interno del sistema dei controlli interni, dei seguenti organi e funzioni con compiti di controllo:
- gli organi aziendali con funzioni di supervisione strategica, gestione e controllo;
- l'O.d.V. eventualmente istituito;
- le funzioni aziendali di conformità alle norme, di controllo dei rischi e di revisione interna;
- i soggetti incaricati della revisione legale dei conti;
- per le banche con azioni quotate, il dirigente preposto alla redazione dei documenti contabili societari ex. art. 154-bis del TUF;

[49] Tale possibilità non ha lo scopo di ridurre gli standard di idoneità preventiva richiesti per i modelli organizzativi, bensì, in modo del tutto coerente con il principio di proporzionalità, quello di semplificare i controlli e alleggerire la struttura di governance nelle società meno complesse, fermi restando tali standard.
[50] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione II, par. 5.

- per le banche con azioni quotate che aderiscono su base volontaria al Codice di autodisciplina della Borsa Italiana, uno o più amministratori incaricati del sistema di controllo interno e di gestione dei rischi e il comitato controllo e rischi.

Affinché il sistema dei controlli interni funzioni correttamente e venga fissato in maniera chiara chi fa che cosa, evitando sovrapposizioni o lacune, è stato, quindi, introdotto l'onere a carico dell'organo con funzione di supervisione strategica di approvare "un documento, diffuso a tutte le strutture interessate, nel quale sono definiti i compiti e le responsabilità dei vari organi e funzioni di controllo, i flussi informativi tra le diverse funzioni/organi e tra queste/i e gli organi aziendali e, nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione"[51].

Le Disposizioni specificano che le banche, nel definire compiti, responsabilità, flussi informativi e modalità di coordinamento/collaborazione di funzioni e organi con compiti di controllo, non possono alterare le responsabilità primarie degli organi aziendali in materia di sistema dei controlli interni.

2.2 Gli elementi innovativi riferibili al controllo dei rischi

Con riferimento alla gestione e al controllo dei rischi, la nuova normativa innova principalmente nei seguenti aspetti:

- il Risk Appetite Framework;
- l'indipendenza e l'autorevolezza delle funzioni aziendali di controllo;
- il coinvolgimento della funzione di compliance;
- i poteri della funzione di controllo dei rischi;
- i compiti della funzione di internal audit;
- l'esternalizzazione delle funzioni aziendali di controllo.

2.2.1 Le novità in materia di Risk Appetite Framework (RAF)

Post crisi, una delle tante debolezze riscontrate nella gestione dei rischi all'interno delle banche è stata individuata nell'incoerenza tra i rischi effettivamente assunti dall'intermediario e quelli percepiti dagli organi aziendali. La principale ragione di tale scarsa consapevolezza è sembrata risiedere nell'insufficiente coinvolgimento di questi ultimi nella definizione del RAF e nel suo monitoraggio. Le stesse definizioni di risk appetite si sono rilevate in molti casi non robuste, non supportate da un adeguato set di misure e incapaci di prevedere azioni specifiche a fronte delle perdite e del superamento dei limiti stabiliti. L'esperienza della crisi ha quindi dimostrato l'importanza di adottare e attuare un RAF come strumento in grado di far convergere l'attenzione dell'intermediario sul suo profilo di rischio. Tale accresciuta attenzione presenterebbe inoltre significative relazioni e sinergie con il processo ICAAP, collocandosi idealmente "a monte" rispetto a quest'ultimo[52].

Con le nuove Disposizioni viene introdotto nell'ordinamento di vigilanza italiano il concetto di Risk Appetite Framework (RAF), o sistema degli obiettivi di rischio o quadro di riferimento per la definizione della propensione al rischio.
Prima di affrontare quanto indicato dalle Disposizioni, appare opportuno sottolineare che la fonte ispiratrice della novità in esame è essenzialmente riconducibile al documento rubricato *Thematic Review on Risk Governance*, pubblicato dal Financial Stability Board (FSB) il 12 febbraio 2013. Rileva notare che si tratta del seguito di un'analisi svolta dallo stesso FSB in occasione di una verifica sul campo (c.d. Peer review Report) circa la robustezza dei sistemi di

[51] *Ibid*.
[52] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.

governance delle banche. Nel documento citato, il FSB evidenzia che, dopo lo scoppio della crisi del 2008, le Autorità di vigilanza nazionali hanno effettivamente adottato nuovi e più efficienti approcci per indurre le banche a mettere in pratica modelli di risk governance prima assenti o comunque deficitari. Nonostante ciò, denuncia il FSB nel suo documento, i progressi raggiunti non erano ancora soddisfacenti. L'indagine ha infatti evidenziato una serie di lacune, specialmente di carattere organizzativo[53].
Sulla base dei risultati della perr review, il FSB ha formulato, nello stesso documento del febbraio 2013, cinque specifiche raccomandazioni e con una di queste ha invitato le autorità di supervisione a fornire guidelines contenenti indicazioni sugli elementi chiave da incorporare in efficaci RAF, con particolare riferimento alla nomenclatura dei concetti utilizzati che deve garantire comparabilità tra i sistemi degli obiettivi di rischio delle istituzioni finanziarie e facilitare la comunicazione tra queste ultime e le Autorità di vigilanza. Il FSB si era impegnato, in tale contesto, a finalizzare l'opera di identificazione di definizioni comuni entro la fine del 2013[54].
In data 18 novembre 2013, il FSB, ha pubblicato il documento rubricato *Principles for An Effective Risk Appetite Framework*, facente parte di una iniziativa dello stesso FSB finalizzata ad aumentare intensità ed efficacia preventiva dell'azione della vigilanza, una delle componenti chiave delle politiche di prevenzione dei rischi approvate dal G20 nel novembre 2010 per affrontare il problema delle imprese a rilevanza sistemica (c.d. SIFIs). Il documento in questione, la cui pubblicazione è successiva a quella del 15° aggiornamento alla Circolare 263/2006, rappresenta una integrazione extragiuridica, assimilabile ad un contributo della prassi, della disciplina di vigilanza in materia di RAF contenuta nel Capitolo 7 della citata circolare[55].
Alla Sezione II ("Key definitions") del documento sopra citato il FSB identifica, ai fini della comprensione dei principi affermati e con l'obiettivo si stabilire una nomenclatura comune per le giurisdizioni e le istituzioni finanziarie, sei definizioni dei termini chiave utilizzati nell'ambito del RAF: Risk appetite framework, Risk appetite statement, Risk capacity, Risk appetite, Risk limits e Risk profile.

Tornando alla normativa nazionale, le Disposizioni declinano il RAF come: "il quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il business model e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli"[56].

Le Disposizioni forniscono, inoltre, come raccomandato dal FSB nei documenti sopra citati, le seguenti definizioni dei concetti rilevanti ai fini del RAF (cfr. Capitolo 7, Sezione I, par. 3):

- risk capacity (massimo rischio assumibile), livello massimo di rischio che una banca è in grado di assumere senza violare i requisiti regolamentari o gli altri vincoli imposti dagli azionisti o dall'autorità di vigilanza;
- risk appetite (obiettivo di rischio o propensione al rischio), livello di rischio (complessivo e per tipologia) che la banca intende assumere per il perseguimento dei suoi obiettivi strategici;
- risk tolerance (soglia di tollerenza), devianza massima dal risk appetite consentita; la soglia di tolleranza è fissata in modo da assicurare in ogni caso alla banca margini sufficienti per operare, anche in condizioni di stress, entro il massimo rischio assumibile; nel caso in cui sia consentita l'assunzione di rischio oltre l'obiettivo di rischio fissato,

[53] Cfr. Metelli F., *FSB: Principles for An Effective Risk Appetite Framework*, articolo tratto dal sito ww.aifirm.it.
[54] Cfr. Financial Stability Board, *Thematic Review on Risk Governance*, Recommendation 4, 12 febbraio 2013.
[55] Cfr. Metelli F., *FSB: Principles for An Effective Risk Appetite Framework*, op. cit.
[56] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 3.

fermo restando il rispetto della soglia di tolleranza, devono essere individuate le azioni gestionali necessarie per ricondurre il rischio assunto entro l'obiettivo prestabilito;

- risk profile (rischio effettivo), rischio effettivamente assunto, misurato in un determinato istante temporale;
- risk limits (limiti di rischio), articolazione degli obiettivi di rischio in limiti operativi, definiti, in linea con il principio di proporzionalità, per tipologie di rischio, unità e/o linee di business, linee di prodotto, tipologie di clienti.

Le definizioni fornite dalle Disposizioni sembrano, quindi, inquadrare il RAF come il quadro di riferimento per la determinazione della propensione al rischio, che, da un alto, funge da strumento per il controllo strategico, nella misura in cui lega i rischi alla strategia aziendale, traducendo la mission e il piano strategico in variabili quali-quantitative, e, dall'altro lato, opera come strumento per la gestione e il controllo dei rischi, in quanto lega gli obiettivi di rischio all'operatività aziendale, traducendoli in vincoli e incentivi per la struttura[57].

La disciplina in materia di RAF si arricchisce anche di ulteriori previsioni normative contenute nell'Allegato C alla citata circolare.

Queste premettono che il RAF deve fissare "ex ante gli obiettivi di rischio/rendimento che l'intermediario intende raggiungere e i conseguenti limiti operativi"[58]. Concettualmente, il RAF, potrebbe, quindi, essere definito come la variabilità dei risultati corretti per il rischio che la banca è disposta ad accettare a fronte di una determinata strategia operativa. In altre parole, l'attività operativa deve svilupparsi all'interno dei limiti di tolleranza al rischio predefiniti[59].

Le previsioni dell'Allegato C sottolineano, anche, che "la formalizzazione, attraverso la definizione del RAF, di obiettivi di rischio coerenti con il massimo rischio assumibile, il business model e gli indirizzi strategici è un elemento essenziale per la determinazione di una politica di governo dei rischi e di un processo di gestione dei rischi improntati ai principi della sana e prudente gestione aziendale"[60].

Se da un lato, la propensione al rischio determinata deve essere coerente con gli indirizzi strategici stabiliti dal board, dall'altro, risulta di fondamentale importanza, integrare i risultati del RAF all'interno della pianificazione strategica. Il profilo di rischio deve, infatti, sempre essere associato al concetto di rendimento. In questo modo la propensione al rischio è integrata nel processo di pianificazione strategica e di budgeting. È, inoltre, necessario misurare i rischi prospettici, incorporando nel piano strategico/ICAAP i risultati delle analisi di scenario, che rivestono un ruolo cruciale nella valutazione della sostenibilità del business. Business model, piano strategico, budget annuali e processo ICAAP, sono tutte premesse logiche per la formalizzazione del RAF che le banche sperimentavano e predisponevano già prima del nuovo impegno imposto agli organi aziendali a partire da gennaio 2014[61].

L'allegato in esame, dopo aver inquadrato in linea generale il RAF, fornisce "indicazioni minimali per la definizione del Risk Appetite Framework, fermo restando che l'effettiva articolazione del RAF va calibrata in base alle caratteristiche dimensionali e di complessità operativa di ciascuna banca"[62]. Tali indicazioni sono riepilogate all'interno del Box 8.

---

[57] Cfr. Marangoni M., *Il provvedimento di Banca d'Italia sul sistema dei controlli interni, impatti e novità*, op. cit.

[58] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Allegato C, par. 1.

[59] Cfr. Metelli F., *Il sistema di controllo e governo dei rischi. Le novità in materia di Risk Appetite Framework, il ruolo di organi e funzioni aziendali*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

[60] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Allegato C, par. 1.

[61] Cfr. Metelli F., *Il sistema di controllo e governo dei rischi. Le novità in materia di Risk Appetite Framework, il ruolo di organi e funzioni aziendali*, op. cit.

[62] Banca d'Italia, *Circ. n. 263 del 27/12/2006, op.* cit., Titolo V, Capitolo 7, Allegato C, par. 2.

Box 8 - *I contenuti minimali del RAF*

In particolare, il RAF (cfr. Capitolo 7, Allegato C, par. 2):

- indica le tipologie di rischio che la banca intende assumere, tenuto conto del piano strategico, dei rischi rilevanti ivi individuati e del massimo rischio assumibile;
- per ciascuna tipologia di rischio, fissa gli obiettivi di rischio, le eventuali soglie di tolleranza e i limiti operativi in condizioni sia di normale operatività, sia di stress;
- indica le circostanze al ricorrere delle quali l'assunzione di determinate categorie di rischio va evitata o contenuta rispetto agli obiettivi e ai limiti fissati;
- definisce le procedure e gli interventi gestionali da attivare al raggiungimento della soglia di tolleranza;
- precisa anche le tempistiche e le modalità da seguire per l'aggiornamento del RAF;
- precisa i compiti degli organi e di tutte le funzioni aziendali coinvolte nella definizione del processo.

I contenuti minimali possono quindi essere identificati negli obiettivi di rischio, nelle soglie di tolleranza (ove definite) e nei limiti di rischio.

Le Disposizioni specificano che obiettivi, soglie e limiti "[…] sono, di norma, declinati in termini di:

a) misure espressive del capitale a rischio o capitale economico (Var, expected shortfall, ecc);
b) adeguatezza patrimoniale;
c) liquidità"[63].

Per quanto riguarda i rischi quantificabili la declinazione degli elementi del RAF, ossia propensione al rischio, soglie di tolleranza e limiti di rischio, deve avvenire attraverso l'utilizzo di opportuno parametri quantitativi e qualitativi, calibrati in funzione del principio di proporzionalità; a tal fine, le banche possono far riferimento alle metodologie di misurazione dei rischi utilizzate ai fini della valutazione dell'adeguatezza patrimoniale (ICAAP). Per quanto concerne, invece, i rischi difficilmente quantificabili, come il rischio strategico e reputazionale, il RAF deve fornire specifiche indicazioni di carattere qualitativo che siano in grado si orientare la definizione e l'aggiornamento dei processi e dei presidi del sistema dei controlli interni (cfr. Capitolo 7, Allegato C, par. 2).

L'AIR definitiva, pubblicata dalla Banca d'Italia nel giugno 2013, evidenzia i benefici e i costi dell'opzione regolamentare adottata.

Le opzioni regolamentari individuate erano le seguenti:

- HO: mantenimento dello status quo, ossia nessuna formalizzazione del livello di rischio assumibile;
- HI: definizione del livello di rischio assumibile;
- H2: individuazione delle variabili quali-quantitative che guidino l'organo con funzione di supervisione strategica nel determinare il massimo livello di rischio assumibile.

Mentre le disposizioni in consultazione accoglievano l'opzione H1 (l'intermediario esplicita il proprio risk appetite), il testo definitivo ha adottato l'opzione indicata in H2 (il risk appetite è definito sulla base di variabili quali-quantitative) che, rispetto alla prima ipotesi, è sicuramente accompagnata da maggiori benefici. Se è del tutto pacifico che l'esplicitazione del risk appetite comporti in capo all'intermediario una maggiore consapevolezza dei rischi assunti da parte degli

[63] *Ibid.*

organi decisionali e un beneficio a livello di sistema finanziario, è, infatti, altrettanto corretto affermare che un RAF efficace presuppone necessariamente l'utilizzo di metriche quantitative e di indicazioni qualitative per la definizione del risk appetite, senza i quali il suo effettivo utilizzo sarebbe pregiudicato e con esso i benefici auspicabili. L'AIR definitiva evidenzia, però, l'impossibilità di identificare in modo puntuale i parametri che gli intermediari dovrebbero utilizzare, anche a motivo dell'esistenza di prassi aziendali molto eterogenee. A fronte di tali benefici, l'AIR definitiva evidenzia costi addizionali per gli intermediari sia nella fase di definizione del framework che in quella di monitoraggio, legati alla necessità di dedicare allo scopo ricorse aggiuntive. Per contro, non si ravvisano costi indiretti né costi diretti per l'Autorità di vigilanza.
L'AIR preliminare, per quanto concerne il RAF, chiedeva, agli intermediari di rispondere a vari quesiti ai fini di una migliore valutazione dell'impatto delle opzioni H1 e H2 in termini di costi e benefici. Veniva chiesto, in particolare, di informare l'Autorità circa la disponibilità da parte degli intermediari di un formale RAF, circa gli organi coinvolti nella sua formalizzazione, attuazione e verifica, circa l'utilizzo di variabili quali-quantitative, e circa i costi connessi alla sua implementazione e all'utilizzo delle suddette variabili.
In merito, dalle risposte pervenute nel corso della consultazione, l'AIR definitiva sostiene che per i grandi intermediari la formalizzazione del RAF dovrebbe comportare costi minori rispetto ai costi che dovrebbero sostenere i piccoli intermediari nell'ambito del sistema del credito cooperativo, i quali hanno evidenziato la mancanza di un framework formale. I costi di adeguamento per i piccoli intermediari sarebbero molto elevati. L'AIR definitiva ritiene, infatti, che la formalizzazione del RAF non comporti solo l'individuazione di soglie e parametri ma anche l'implementazione di procedure, di strumenti di monitoraggio e l'attivazione di vincoli e incentivi.
Le Disposizioni contenute nell'Allegato C, infatti, aprono il par. 2 rubricato "Indicazioni sul contenuto del RAF" specificando che l'effettiva articolazione del RAF deve essere calibrata in base alla dimensione e alla complessità di ciascuna banca, nel rispetto, quindi del principio di proporzionalità.

2.2.2 L'indipendenza e l'autorevolezza delle funzioni aziendali di controllo: istituzione, programmazione, rendicontazione e collaborazione

Tra gli argomenti di natura meno tecnica contenuti nel Capitolo 7, Titolo V, Circolare 263/2006, ma certamente di rilievo e quindi degni di approfondimento, vi sono le previsioni contenute nella Sezione III relative all'istituzione, programmazione e rendicontazione delle funzioni aziendali di controllo (parr. 1 e 2), alle responsabilità e ai compiti di ciascuna funzione (parr. 3.1, 3.2, 3.3), e ai rapporti tra le funzioni aziendali di controllo e le altre funzioni aziendali (par. 3.5).

Il contenuto della sezione in esame è lo sviluppo coerente dei principi generali contenuti nelle disposizioni preliminari sul sistema dei controlli interni di cui alla Sezione I del Capitolo 7, già oggetto di approfondimento al par. 1.3 del Capitolo 1.

In continuità con le previsioni di natura più generale e al fine di presidiarne la concreta attuazione, la Sezione III del Capitolo 7 dedica al tema dell'istituzione un intero paragrafo rubricato "Istituzione delle funzioni aziendali di controllo" (par. 1) all'interno del quale la Banca d'Italia stabilisce chiare e rigorose disposizioni concernenti l'istituzione e l'indipendenza, anche organizzativa e nell'esercizio dell'attività, delle funzioni aziendali di controllo, nonché la procedura di nomina e i requisiti di professionalità richiesti in capo ai relativi responsabili.

Prima di definire requisiti e oneri, la Banca d'Italia stabilisce che le banche devono istituire, secondo quanto indicato dalla sezione in questione e ferma restando l'autonoma responsabilità aziendale per le scelte effettuate in materia di assetto dei controlli interni,

"funzioni aziendali di controllo permanenti e indipendenti: i) di conformità alle norme (compliance); ii) di controllo dei rischi (risk management); iii) di revisione interna (internal audit)"[64].

Per assicurare l'indipendenza delle funzioni aziendali di controllo dalle aree di business e tra le stesse funzioni, le Disposizioni stabiliscono che (cfr. Capitolo 7, Sezione III, par. 1):

a) le stesse funzioni devono disporre dell'autorità, delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti; possono avere accesso ai dati aziendali e a quelli esterni; devono disporre di risorse economiche, attivabili anche in autonomia, che gli permettono, tra l'altro, di ricorrere a consulenze esterne; devono godere di un personale adeguato per numero, competenze e aggiornamento; devono essere inserite in programmi di formazione e di rotazione delle risorse tra le stesse funzioni aziendali di controllo, in modo da garantire la formazione di competenze trasversali e acquisire una visione integrata dell'attività di controllo;
b) i responsabili delle funzioni devono possedere i requisiti di professionalità adeguati; devono collocarsi in posizione gerarchico – funzionale adeguata; non devono avere responsabilità diretta di aree operative sottoposte a controllo, né essere subordinati ai responsabili di tali aree; devono essere nominati e revocati dall'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo; possono essere componenti dell'organo amministrativo purché destinatari di deleghe in materia di controlli e non di altre deleghe che potrebbero pregiudicarne l'autonomia; riferiscono direttamente agli organi aziendali;
c) il personale partecipante alle funzioni aziendali di controllo non deve essere coinvolto in attività controllate dalle stesse funzioni;
d) le funzioni aziendali di controllo devono essere tra loro separate dal punto di vista organizzativo e i rispettivi ruoli e responsabilità devono essere formalizzati;
e) i criteri di remunerazione del personale partecipante alle funzioni aziendali di controllo non devono comprometterne l'obiettività, bensì concorrere alla creazione di un sistema di incentivi coerente con le finalità della funzione.

Da segnalare, tra i requisiti stabiliti per assicurare l'indipendenza delle funzioni, che la nomina dei responsabili delle funzioni aziendali di controllo, da attuarsi previa selezione dei candidati in base a procedure debitamente formalizzate, rientra tra le dirette responsabilità dell'organo di supervisione strategica, sentito l'organo di controllo.

Circa i requisiti, i responsabili delle funzioni di controllo devono possedere caratteristiche di professionalità adeguate allo specifico ruolo e coerenti rispetto ai profili individuati per la funzione, tenendo conto del sopra citato processo formalizzato di selezione. Una scrupolosa selezione dei profili più professionalmente adeguati a ricoprire i ruoli apicali nell'ambito delle funzioni aziendali di controllo è, infatti, una delle condizioni individuate per assicurare alle stesse un'effettiva indipendenza, unitamente alle specifiche e dettagliate previsioni afferenti le prerogative e i poteri di intervento e verifiche in capo alle suddette funzioni e la loro collocazione gerarchico – funzionale. In altri termini, ad un sistema di regole di funzionamento capace di fornire e garantire alle funzioni i più idonei strumenti di intervento, valutazione ed analisi, devono corrispondere le competenze necessarie allo svolgimento dei compiti assegnati. Con riferimento in particolare agli strumenti è previsto che le funzioni di controllo abbiano esteso accesso ai dati aziendali, disponibilità economiche attivabili anche in economia per l'eventuale ricorso a consulenze esterne, risorse umane adeguate e percorsi di formazione atti a sviluppare nel continuo le competenze tecnico-professionali[65].

[64] Banca d'Italia, *Circ. n. 263 del 27/12/2006 ,op.* cit., Titolo V, Capitolo 7, Sezione III, par. 1.

[65] Cfr. Priori M., Guglielmetti R., *Istituzione e nomina delle funzioni di controllo*, in Osservatorio di diritto bancario del Sole 24 ORE, 19 novembre 2013.

Relativamente alla collocazione gerarchico – funzionale, è previsto che i responsabili delle funzioni di controllo di 2° livello possano essere posizionati alle dirette dipendenze dell'organo con funzione di gestione o dell'organo con funzione di supervisione strategica, mentre il responsabile della revisione interna deve sempre essere collocato alle dirette dipendenze dell'organo con funzione di supervisione strategica, fermo restando che tutti i responsabili non devono avere responsabilità diretta di aree operative né essere gerarchicamente subordinati ai responsabili di tali aree (cfr. Capitolo 7, Sezione III, par. 1).
Per quanto concerne la collocazione delle funzioni aziendali di controllo di 2° livello, l'Autorità di vigilanza ha espressamente stabilito, nell'ambito della Nota di chiarimenti del 24/01/2014, successivamente aggiornata in data 06/06/2014, che nelle banche di piccole dimensioni o a limitata complessità operativa, sprovviste di un amministratore delegato e di un comitato esecutivo, le stesse funzioni non possono essere collocate a riporto gerarchico del D.g., bensì devono essere collocate alle dirette dipendenze dell'organo con funzione di gestione, che in questi casi è da individuarsi nell'organo con funzione di supervisione strategica[66].
L'aggiornamento del 06/06/2014 ha inoltre precisato che risulta ammissibile collocare i responsabili delle funzioni aziendali di controllo di 2° livello a riporto gerarchico di un solo componente dell'organo amministrativo solo se tale amministratore è identificabile con l'organo con funzione di gestione, ossia solo quest'ultimo riveste il ruolo di amministratore delegato.

Da ultimo, ma non certo per importanza, è previsto che le funzioni di controllo riferiscano direttamente agli organi aziendali. In particolare, i responsabili delle funzioni di conformità alle norme e di controllo dei rischi hanno accesso diretto agli organi con funzione di supervisione strategica e con funzione di controllo e comunicano con essi senza restrizioni o intermediazioni; il responsabile della revisione interna ha accesso diretto all'organo con funzione di controllo e comunica con esso senza restrizione o intermediazione alcuna (cfr. Capitolo 7, Sezione III, par. 1). In questo modo è assicurata la loro autonomia funzionale e incisività d'azione in rapporto diretto con i massimi organi di governo societario, primi interessati all'adeguatezza e affidabilità del sistema dei controlli interni[67].

Le Disposizioni, dopo aver stabilito i requisiti dei responsabili, organizzativi e del personale, si preoccupano di dare risalto al ruolo della proporzionalità, stabilendo che le banche, a condizione che i controlli sui rischi continuino ad essere efficaci, possono affidare a un'unica struttura lo svolgimento della funzione di conformità alle norme e della funzione di controllo dei rischi e/o affidare lo svolgimento delle funzioni aziendali di controllo all'esterno, secondo quanto previsto dalle Sezioni IV e V recanti disposizioni in materia di esternalizzazione al di fuori e all'interno dei gruppi bancari (cfr. Capitolo 7, Sezione III, par. 1).

Infine le Disposizioni, tenuto conto che le funzioni di compliance e di risk managemt sono sottoposte periodicamente a verifica da parte della funzione di internal audit e per assicurare l'imparzialità dei controlli di audit sulle altre funzioni di controllo, stabiliscono che "le funzioni di conformità alle norme e di gestione dei rischi non possono essere affidate alla funzione di revisione interna"[68].

Le richiamate previsioni, contenute nel primo paragrafo della sezione in esame, non apportano particolari novità regolamentari con riguardo alle modalità di istituzione delle funzioni aziendali di controllo e ai relativi requisiti di professionalità e indipendenza. Tuttavia è

[66] Come affermato nel par. 2.1.2, il D.g., pur partecipando alla funzione di gestione, non può essere identificato con l'organo stesso. La Nota del 2014 specifica, inoltre, che il D.g., nei casi prospettati, proprio perché rappresenta il vertice della struttura interna e partecipa alla funzione di gestione, può svolgere un ruolo di raccordo funzionale tra le funzioni aziendali di controllo di 2° livello e l'organo con funzione di gestione, da cui dipendono gerarchicamente le citate funzioni.
[67] Cfr. Priori M., Guglielmetti R., *Istituzione e nomina delle funzioni di controllo*, op. cit.
[68] Banca d'Italia, *Circ. n. 263 del 27/12/2006, op.* cit., Titolo V, Capitolo 7, Sezione III, par. 1.

possibile segnalare che le banche, rispetto al previgente contesto normativo di riferimento, dovranno procedere, come già sopradetto, alla formalizzazione, o alla verifica, dei regolamenti concernenti le procedure di selezione dei responsabili delle funzioni aziendali di controllo e dei programmi di rotazione delle risorse tra le funzioni di controllo interno[69].

Anche le previsioni di cui al par. 2 della sezione in esame, rubricato "Programmazione e rendicontazione dell'attività di controllo", non apportano particolari novità rispetto alla previgente normativa di riferimento.

La novità di maggior rilievo riguarda l'obbligatorietà per tutte le funzioni aziendali di controllo, per le materie di rispettiva competenza, di riferire annualmente agli organi aziendali in ordine alla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni[70], oltre a presentare, agli stessi organi aziendali e con cadenza sempre annuale, una relazione dell'attività svolta, che illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati e propone gli interventi da adottare per la loro rimozione (cfr. Capitolo 7, Sezione III, par. 2).

Per quanto concerne la programmazione dell'attività di controllo le Disposizioni specificano che (cfr. Capitolo 7, Sezione III, par. 2):

- le funzioni di controllo di 2° livello, ciascuna secondo le proprie competenza, devono presentare agli organi aziendali, con cadenza annuale, un programma di attività che identifichi e valuti i principali rischi a cui la banca è esposta e programmi gli interventi di gestione;
- la funzione di controllo di 3° livello deve presentare annualmente un piano di audit che indichi le attività di controllo pianificate e contenga una specifica sezione relativa all'ICT auditing.

Infine, le Disposizioni segnalano che in ogni caso, le funzioni aziendali di controllo devono informare tempestivamente gli organi aziendali su ogni violazione o carenza rilevante riscontrata (cfr. Capitolo 7, Sezione III, par. 2).

Le previsioni di cui al par. 3.5 della sezione in esame, rubricato "Rapporti tra le funzioni aziendali di controllo e altre funzioni aziendali", disciplinano i rapporti e i flussi informativi tra le funzioni aziendali di controllo.

Fermo restando la reciproca indipendenza e i rispettivi ruoli, le previsioni stimolano a rafforzare la collaborazione. Stabiliscono, infatti, che le funzioni aziendali di controllo devono collaborare tra loro e con le altre funzioni allo scopo di sviluppare le proprie metodologie di controllo in modo coerente con le strategie e l'operatività aziendale (cfr. Capitolo 7, Sezione III, par. 3.5).

In merito all'articolazione dei flussi informativi le Disposizioni stabiliscono che (cfr. Capitolo 7, Sezione III, par. 3.5):

- i responsabili delle funzioni di 2° livello devono informare il responsabile della funzione di revisione interna delle criticità rilevate nelle proprie attività di controllo che possono essere di interesse per l'attività di audit;
- il responsabile della funzione di 3° livello deve, invece, informare i responsabili delle funzioni di 2° livello delle inefficienze, debolezze o irregolarità emerse nel corso delle attività di audit e relative a aree o materie di loro competenza.

Inoltre, viene espressamente previsto che i compiti e le responsabilità delle diverse funzioni aziendali di controllo siano comunicati all'interno dell'organizzazione aziendale, con particolare riferimento alla suddivisione delle competenze relative alla misurazione dei rischi, alla consulenza in materia di adeguatezza delle procedure di controllo e alle attività di verifica delle procedure medesime (cfr. Capitolo 7, Sezione III, par. 3.5).

[69] Cfr. Fumagalli M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, op. cit.

[70] *Ibid*.

2.2.3 Le novità in materia di coinvolgimento della funzione di compliance e di gestione e controllo del rischio fiscale

L'inserimento organico della funzione di compliance nelle disposizioni che regolano il sistema dei controlli interni e in particolare le funzioni di controllo, deve essere considerato un elemento innovativo di cruciale importanza, in quanto, non solo assicura un quadro unitario per gli operatori bancari, ma rappresenta anche il risultato di scelte importanti su punti critici riguardanti la funzione stessa (in particolare i rapporti con altre funzioni specialistiche come ad es. legale, fiscale ecc.)[71].

Nell'ambito della disciplina sulla conformità alle norme, rimane ferma, tra le altre cose, la definizione di rischio di non conformità alle norme o rischio di compliance contenuta nelle abrogate disposizioni in materia emanate dalla Banca d'Italia nel luglio 2007, che hanno costituito la cornice di riferimento della nuova normativa.
Viene inoltre ribadita, come affermato dalle disposizioni del 2007, la necessità di responsabilizzare adeguatamente tutto il personale della banca, a motivo del fatto che il rischio di compliance è diffuso a tutti i livelli dell'organizzazione aziendale, soprattutto nell'ambito delle linee operative, primo luogo in cui il rischio viene generato e quindi primo luogo in cui l'attività di prevenzione deve svolgersi. Rimane fermo, inoltre, l'approccio risk based che deve guidare la funzione di conformità alle norme, il cui compito specifico è quello di presiedere alla gestione del rischio di compliance a tutti i livelli dell'organizzazione e dell'attività aziendale, verificando che le procedure interne siano idonee a prevenire tale rischio. A tal fine, la funzione di conformità deve avere accesso a tutte le attività della banca, anche quelle periferiche, e a qualsiasi informazione rilevante, anche attraverso colloqui diretti con il personale[72].

Per quanto riguarda i compiti assegnati alla funzione in esame[73], la nuova normativa riprende nella sostanza quanto già stabilito dalle disposizioni della Banca d'Italia del 2007 intrudendo, però, alcune importati novità mostrate all'interno del Box 9.

Box 9 - *Le novità relative alla funzione di compliance*

La nuova disciplina in materia di rischio di non conformità alle norme innova principalmente con riferimento ai seguenti aspetti:

- l'inserimento organico della funzione compliance nelle disposizioni che regolano le funzioni di controllo e più in generale il sistema dei controlli interni;
- l'attribuzione alla funzione di compliance del ruolo di presiedere alla gestione del rischio di non conformità di tutta l'attività aziendale;
- l'inserimento nel perimetro della funzione di non conformità alle normativa di natura fiscale;
- la gradualità del presidio della funzione di compliance[74].

La novità più significativa apportata dalle Disposizioni è sicuramente riscontrabile nell'estensione del perimetro di competenza della funzione di compliance all'intera attività aziendale e quindi a tutte le disposizioni applicabili alle banche, incluse quelle di natura fiscale, seppure prevedendone un coinvolgimento graduato in base al rischio considerato.

---

[71] Cfr. Cola C., *Le novità per la funzione di compliance e la gestione ed il controllo del rischio fiscale*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.
[72] Cfr. Marangoni M., *Il provvedimento di Banca d'Italia sul sistema dei controlli interni, impatti e novità*, op. cit.
[73] Per un completo approfondimento dei compiti assegnati alla funzione di compliance si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione III, par. 3.2.
[74] Cfr. Cola C., *Le novità per la funzione di compliance e la gestione ed il controllo del rischio fiscale*, op. cit.

In particolare, il coinvolgimento della funzione di compliance è graduato sia in relazione al rilievo che le singole norme hanno per l'attività svolta e per le conseguenze della loro violazione, quali quelle che riguardano l'esercizio dell'attività bancaria, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e più in generale la disciplina posta a tutela del consumatore, sia in relazione all'esistenza all'interno della banca di altre forme di presidio specializzato a fronte del rischio di non conformità relativo a specifiche normative (ad es. normativa sulla sicurezza sul lavoro e in materia di trattamento di dati personali).
Per quanto concerne la gestione del rischio di compliance relativo alle norme di maggior rilievo sopra elencate, prevale la responsabilità diretta della funzione in esame, mentre viene disposta dalle Disposizioni la responsabilità condivisa e il coinvolgimento graduato della stessa funzione per le normative con presidio specializzato, previa valutazione dell'adeguatezza dei controlli specialistici posti in essere per gestire i rischi di non conformità alle normative specifiche. In base agli esiti di tale valutazione vengono definiti i compiti della funzione di compliance.
Le Disposizioni prevedono, infatti, che "per le norme più rilevanti […], e per quelle norme per le quali non siano già previste forme di presidio specializzato all'interno della banca, la funzione è direttamente responsabile della gestione del rischio di non conformità", mentre "con riferimento ad altre normative per le quali siano già previste forme specifiche di presidio specializzato […], la banca, in base a una valutazione dell'adeguatezza dei controlli specialistici a gestire i profili di rischio di non conformità, può graduare i compiti della compliance, che comunque è responsabile, in collaborazione con le funzioni specialistiche incaricate, almeno della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità"[75].
L'approccio della gradualità del coinvolgimento può essere adottato, secondo quanto disposto dalle Disposizioni, anche relativamente al presidio del rischio di non conformità alla normativa di natura fiscale, che "richiede almeno: i) la definizione di procedure volte a prevenire violazioni o elusioni di tale normativa e ad attenuare i rischi connessi a situazioni che potrebbero integrare fattispecie di abuso del diritto […], ii) la verifica dell'adeguatezza di tali procedure e della loro idoneità a realizzare effettivamente l'obiettivo di prevenire il rischio di non conformità"[76].
Tale previsione appare al momento opportuna, considerato che, in strutture complesse, dove esistono una pluralità di soggetti che si occupano sotto diversi profili della materia fiscale (ad es. ufficio fiscale, collegio sindacale, O.d.V.), attenua i rischi di sovrapposizioni e di conflitti anche interpretativi tra funzioni, mentre, in strutture meno complesse attenua la criticità della funzione di conformità di non disporre di competenze specialistiche e di dover ricorrere a onerosi supporti consulenziali esterni. In ogni caso alla funzione di compliance è assegnato un presidio che comporta difficoltà sul piano delle competenze professionali e delle risorse disponibili[77].
Le Disposizioni specificano in nota che le procedure da definire possono prevedere il ricorso a figure interne esperte in materia fiscale o, nei casi più complessi, l'acquisizione del parere delle competenti autorità tributarie. Inoltre, precisano che, oltre alla prevenzione dei rischi derivanti dalla mancata osservanza delle normative fiscali, è necessario tenere in considerazione anche l'effettuazione da parte della clientela di operazioni fiscalmente irregolari.

L'AIR definitiva, pubblicata dalla Banca d'Italia nel giugno 2013, evidenzia i benefici e i costi dell'opzione regolamentare adottata.
Le opzioni regolamentari individuate erano le seguenti:

[75] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione III, par. 3.2.
[76] *Ibid*.
[77] Cfr. Cola C., *Le novità per la funzione di compliance e la gestione ed il controllo del rischio fiscale*, op. cit.

- HO: mantenimento dello status quo, ossia incertezza interpretativa circa l'estensione del perimetro di competenza della funzione di compliance;
- HI: interpretazione del perimetro di competenza della funzione di compliance come esteso all'intera attività aziendale;
- H2: interpretazione del perimetro di competenza della funzione di compliance come esteso all'intera attività aziendale, con graduazione del coinvolgimento della funzione in base al rischio considerato.

Le disposizioni poste in consultazione accoglievano l'opzione H1, prevedendo in particolare la responsabilità diretta della compliance anche in relazione al rischio di non conformità alla normativa fiscale. Nel corso della consultazione è emersa una particolare preoccupazione dei rispondenti in ordine all'estensione del perimetro di competenza della funzione di compliance a tutta la normativa potenzialmente applicabile e quindi anche alla normativa fiscale, con particolare riferimento alle operazioni fiscalmente irregolari poste in essere dalla clientela. Sono state inoltre espresse preoccupazioni generali inerenti i costi di adeguamento per gli intermediari. Pertanto, grazie ad una più attenta ponderazione degli effetti collegati alla scelta delle opzioni, guidata dalle risultanze della consultazione, il testo definitivo ha preferito adottare l'approccio della gradualità del coinvolgimento della funzione di compliance, mantenendo comunque l'estensione della competenza a tutta l'attività aziendale.

I benefici connessi all'ampliamento del perimetro di competenza della funzione di compliance riguardano non solo le banche e gli investitori/risparmiatori, ma anche il sistema economico. Il maggior raggio di azione della funzione e la predisposizione di procedure per la prevenzione del rischio di non conformità mitigano i rischi in termini di conseguenze a livello sanzionatorio, producendo, quindi, maggiore efficacia in termini di tutela della legalità dell'attività svolta e di protezione del rischio reputazionale. Inoltre, il coinvolgimento graduato della compliance nell'attività di presidio della normativa fiscale e delle normative che già prevedono figure specializzate di garanzia contribuisce al rafforzamento dei presidi esistenti.

A fronte di tali benefici i costi per gli intermediari sono essenzialmente di natura operativa e legati alla predisposizione delle procedure di mitigazione del rischio rilevato. In tale ambito, la previsione del ruolo della compliance nella predisposizione delle stesse, ma non nella loro attuazione, permette di evitare duplicazioni e sovrapposizioni di attività, richiedendo solo un coordinamento delle stesse. Non si ravvisano costi diretti per l'Autorità di vigilanza.

Per quanto concerne il profilo organizzativo, stante i molteplici profili professionali richiesti per l'espletamento degli adempimenti imposti, le Disposizioni mantengono la previsione contenuta nelle disposizioni del 2007, in base alla quale è possibile affidare le varie fasi dell'attività della funzione di compliance a strutture organizzative già presenti in banca (ad es., legale, organizzazione, gestione del rischio operativo), assicurando, però, che il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità attraverso la nomina di un responsabile che coordini e sovraintenda alle diverse attività.

2.2.4 Il rafforzamento dei poteri della funzione di controllo dei rischi

Le Disposizioni attribuiscono alla funzione di controllo dei rischi la finalità di "collaborare alla definizione e all'attuazione del RAF e delle relative politiche di governo dei rischi, attraverso un adeguato processo di gestione di rischi"[78].

Dal punto di vista organizzativo la nuova disciplina stabilisce che devono essere individuate soluzioni idonee a perseguire in maniera efficiente ed efficace tale obiettivo. L'organizzazione della funzione di controllo dei rischi deve, a tal fine, rispettare i seguenti principi (cfr. Capitolo 7, Sezione III, par. 3.3):

[78] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione III, par. 3.3.

- può essere variamente articolata (ad es, in relazione ai singoli profili di rischio), purché venga mantenuta una visione d'insieme dei rischi a cui la banca è sottoposta e delle loro interazioni;
- se coerente con il principio di proporzionalità, le banche che adottano sistemi interni per la misurazione dei rischi, devono individuare all'interno della funzione in esame unità preposte alla convalida di detti sistemi e assicurare la loro indipendenza dalle unità responsabili dello sviluppo degli stessi;
- può prevedere, soprattutto nelle banche complesse, la costituzione di specifici comitati di gestione dei diversi profili di rischio; laddove questi comitati siano istituiti è necessario verificare che ciò non depotenzi le prerogative del risk management; le soluzioni organizzative individuate non devono determinare una eccessiva distanza dal contesto operativo, dato che per la piena consapevolezza dei rischi è necessario che vi sia una continua interazione critica con le unità di business.

Una delle principali novità introdotte dalle Disposizioni consiste nel rafforzamento dei poteri della funzione di risk management. Le Diposizioni apportano, infatti, numerose modifiche rispetto a quanto previsto dalla previgente normativa in materia di risk management, segnalate all'interno del Box 10.

Box 10 - *I nuovi poteri/compiti della funzione di controllo dei rischi*

Sono stati introdotti ulteriori ambiti di competenza della funzione di risk management che riguardano, oltre ai compiti di ausilio all'organo con funzione di supervisione strategica nella definizione del RAF e all'attuazione e alla verifica dello stesso, anche i seguenti aspetti (cfr. Capitolo 7, Sezione III, par. 3.3):

- ❖ lo sviluppo e l'applicazione di indicatori in grado si segnalare situazioni di anomalia ed inefficienze dei sistemi di misurazione e controllo dei rischi, cosiddetti indicatori di anomalia;
- ❖ l'analisi dei rischi connessi a nuovi prodotti/servizi e all'ingresso in nuovi segmenti/mercati;
- ❖ il rilascio di pareri preventivi sulla coerenza con il RAF delle operazioni di maggior rilevo; in caso di parere negativo, la decisione sull'operazione è rimessa all'organo con funzione di gestione;
- ❖ la verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni creditizie[79].

Il ruolo del CRO (Chief Risk Officer) è stato, quindi, significativamente ampliato. Tra i nuovi compiti affidati al CRO rileva particolarmente il potere di verificare il corretto svolgimento del monitoraggio andamentale sulle esposizioni creditizie, e il potere di vagliare preventivamente le operazioni di maggior rilievo, c.d. potere di veto, con possibilità di attivare procedure di escalation verso l'esecutivo aziendale[80].

Per quanto concerne la verifica del corretto svolgimento del monitoraggio andamentale sulle esposizioni creditizie, la Banca d'Italia ha espressamente stabilito, nell'ambio della già richiamata Nota del 24/01/2014 aggiornata il 06/06/2014, che, ove esistessero strutture che già effettuano un controllo di 2° livello sul monitoraggio andamentale del credito, ai fini del rispetto della nuova normativa, queste devono essere collocate a riporto gerarchico del responsabile del risk management.

[79] Cfr. *Fumagalli M., Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, op. cit.

[80] Cfr. Banca d'Italia, *Sintesi per gli utenti. Nuove disposizioni di vigilanza prudenziale per le banche (Circ. n. 263 del 27 dicembre 2006) – 15° aggiornamento Sistema dei controlli interni, sistema informativo e continuità operativa*, 24 gennaio 2014.

I criteri e le procedure di controllo andamentale e di monitoraggio delle singole esposizioni creditizie, sono regolate dalle previsioni di cui al par. 2 dell'Allegato A alla Circolare 263/2006[81]. Le Disposizioni, infatti, nell'affidare al risk management l'importante ruolo di verifica sul monitoraggio delle esposizioni creditizie, rimandano alle previsioni contenute nell'allegato sopradetto, le quali stabiliscono che: "la verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni, in particolare di quelle deteriorate, e la valutazione della coerenza delle classificazioni, della congruità degli accantonamenti e dell'adeguatezza del processo di recupero è svolta, […], dalla funzione di controllo dei rischi o, per le banche di maggiore dimensione o complessità operativa, da una specifica unità, che riporta al responsabile della funzione di controllo dei rischi. Tali unità verificano, tra l'altro, l'operato delle unità operative e di recupero crediti, assicurando la corretta classificazione delle esposizioni deteriorate e l'adeguatezza del relativo grado di irrecuperabilità. Nel caso di valutazioni discordanti, si applicano le valutazioni formulate dalla funzione di controllo dei rischi"[82].

Tali nuove previsioni richiederanno alle banche di modificare la regolamentazione interna della funzione in esame, oltre che rivedere ed eventualmente integrare le metodologie di lavoro adottate per adeguarle alle nuove previsioni.

La necessità di rafforzare i poteri della funzione di controllo dei rischi e il ruolo del CRO, come specificato dalla Banca d'Italia nell'AIR definitiva del 2013, nasce dai principali elementi di criticità che hanno riguardato la stessa funzione negli anni più recenti: il rango organizzativo e l'indipendenza del CRO, spesso insufficienti e inadeguati a consentire un corretta valutazione ex ante degli effetti sulla rischiosità delle scelte aziendali, e l'assenza di una regolare interazione con il Board e di un rapporto di parità dialettica con gli altri senior manager. La Banca d'Italia, nella sua relazione sull'analisi d'impatto della nuova regolamentazione, ricorda che a livello internazionale, l'indipendenza del CRO e il reporting diretto al Board rientrano tra le raccomandazioni e i principi definiti da più organismi[83].
Prima di relazionare sui costi e i benefici delle opzioni regolamentari individuate, la Banca d'Italia afferma nell'AIR definitiva, a conclusione di queste prime considerazioni, che Il CRO, e più in generale il risk management, dovrebbe avere la struttura organizzativa, la capacità e l'autorità necessarie per assicurare che gli organi di vertice siano informati sul profilo di rischio e sulle questioni di rischio maggiormente rilevanti in modo tempestivo e regolare.
Il perseguimento di queste finalità hanno spinto l'Autorità di vigilanza a individuare tre opzioni regolamentari, riassunte dall'AIR definitiva nelle seguenti:

[81] L'Allegato A alle Disposizioni, rubricato "Disposizioni speciali relative a particolari categorie di rischio", è interamente dedicato a specifiche categorie di rischio per le quali riporta linee guida in materia di controlli interni, fermo restando quanto previsto nelle specifiche discipline relative alle stesse. Si ritiene opportuno, in questa sede, non approfondire quanto stabilito dalle previsioni citate in materia di controllo andamentale e, più in generale, dell'intero processo di gestione del rischio di credito e di controparte, essendo sufficiente, ai fini della comprensione dell'accrescimento delle competenze in capo al risk management, sottolineare il nuovo ruolo attribuito in questo ambito alla funzione in esame. Per ulteriori approfondimenti si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, Titolo V, Capitolo 7, Allegato A.

[82] Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Allegato A.

[83] Si citano, a titolo esemplificativo: la Commissione Europea, che, nel *Libro Verde* del 2010 dedicato alla corporate governance nelle istituzioni finanziarie e alle politiche di remunerazione, ha sottolineato come il fallimento del risk management sia dipeso anche da mancanza di autorità di questa funzione e da un sistema di comunicazione e informazione sui rischi sostanzialmente povero; l'EBA, che, nelle sue *Guidelines on Internal Governance* pubblicate nel 2011, assume un posizione ancora più incisiva fornendo la possibilità agli intermediari di concedere alla figura del CRO un diritto di veto, previa definizione delle circostanze in cui esso può essere esercitato e delle modalità con cui verrebbe informato l'organo con funzione di gestione; il FSB, che, nell'ambito del Perr review Report *Thematic review on risk governnace* pubblicato nel febbraio 2013, ha identificato le best practice con riguardo alle caratteristiche e al funzionamento della funzione risk management e ha esortato le autorità di regolamentazione e di supervisione a promuoverle (cfr. Recommendation 1).

- HO: mantenimento dello status quo, quindi nessun obbligo della risk management function di pronunciarsi preventivamente sulle operazioni di maggior rilievo;
- HI: la banca ha la facoltà di conferire alla funzione in esame il compito di esaminare preventivamente le operazioni maggior rilievo; la funzione è tenuta a riferire al Board nel caso in cui tali operazioni non siano compatibili con le politiche di rischio definite;
- H2: la funzione di risk management deve pronunciarsi ex ante sulle operazioni di maggior rilevo nel rispetto dei criteri stabiliti dall'organo con funzione di supervisione strategica; è tenuta a riferire al Board l'incompatibilità di talune operazioni con le politiche di rischio dell'intermediario.

Le Disposizioni, come noto, sono coerenti con l'opzione H2 nella misura in cui prevedono che la funzione in esame pronunci pareri preventivi sulla coerenza delle operazioni di maggior rilievo con la politica aziendale di governo dei rischi. In caso di parere negativo, la decisione sull'operazione sarebbe rimessa all'organo con funzione di gestione, che informerebbe quello con funzione di supervisione strategica e l'organo con funzione di controllo. La procedura informativa sopradetta è definita di escalation. Anche la normativa in consultazione accoglieva la stessa opzione.

L'opzione adottata presenta il beneficio di portare sempre l'attenzione degli organi decisionali sulle operazioni con effetto significativo sulla stabilità dell'intermediario. Gli effetti positivi che ne discendono riguardano anche l'intero sistema finanziario e il buon funzionamento dell'economia. A fronte di tali benefici, oltre al possibile rallentamento del processo decisionale, possono essere ipotizzati costi di impianto per le singole banche, connessi con l'individuazione da parte dell'organo con funzione strategica delle operazioni di maggior rilievo che sarebbero oggetto di vaglio preventivo da parte della funzione di risk management . Per contro, i costi ricorrenti varierebbero in relazione alle modalità di individuazione delle operazioni in questione.

L'AIR definitiva specifica, a tale riguardo, che, per l'identificazione delle operazioni di maggior rilevo, possono essere distinte le seguenti sub-opzioni regolamentari:

i. utilizzo di variabili quantitative assolute e/o relative;
ii. utilizzo di criteri qualitativi;
iii. valutazione in autonomia della rilevanza dell'operazione.

L'utilizzo di variabili quantitative e qualitative renderebbe più agevole tale individuazione e comporterebbe costi più bassi. Tuttavia tale tipo di identificazione si tradurrebbe in una minore flessibilità.

L'AIR preliminare, per quanto concerne le OMR, chiedeva, agli intermediari di rispondere a vari quesiti ai fini di una migliore valutazione dei costi e dei benefici delle opzioni regolamentari disponibili. Veniva chiesto, in particolare, di informare l'Autorità circa la previsione da parte degli intermediari di un'azione di controllo preventivo della funzione di controllo dei rischi, circa l'opinione degli stessi in merito alla possibilità di riconoscere, laddove non già previsto, un tale ruolo, circa i rischi di attuazione e i costi di una tale previsione.

In sede di consultazione, è emerso che i costi di implementazione sono considerati dai piccoli intermediari elevati e legati alle attività di individuazione delle operazioni di maggior rilievo, di consulenza e formazione. I grandi intermediari, invece, sostengono che i costi dipenderebbero dal punto di partenza dell'istituzione e dalla natura del controllo preventivo delle operazioni.

In merito, dalle risposte pervenute in sede di consultazione emerge un quadro eterogeneo: i piccoli intermediari sottolineano che in genere non c'è un controllo preventivo della risk management function, mentre i grandi intermediari denunciano un controllo non stabilmente generalizzato ex ante, ma deciso su base occasionale. Una generalizzata attribuzione del ruolo in esame alla funzione di controllo dei rischi è, comunque, valutata positivamente da entrambe le categorie di banche. Tuttavia, se da un lato i grandi intermediari non segnalano particolari rischi di attuazione, dall'altro i piccoli intermediari sottolineano che l'attribuzione di un potere

di veto alla funzione di risk management non sarebbe esente da rischi, quali, tra gli altri, il solo rispetto formale, il conflitto tra organi e il rallentamento dell'attività.

2.2.5 Le principali novità in tema di Internal audit

La funzione di revisione interna, prima del XV° aggiornamento alla Circolare 263/2006, trovava la propria disciplina nelle *Istruzioni di vigilanza per le banche* del 1999. La previgente normativa di vigilanza delineava una figura avente le caratteristiche sia del supervisore che del consulente. Emerge, quindi, la natura composita dell'attività di audit: la normativa tratteggiava una funzione dedita al controllo tanto quanto alla consulenza, attenta ad individuare i problemi tanto quanto la soluzione di essi. A fronte delle carenze riscontrate, l'Internal audit concorre, infatti, al processo di crescita aziendale fornendo proposte per ottimizzare politiche, procedure e metodologie di lavoro. Pertanto, l'auditing è una rete di protezione aziendale ed insieme uno strumento di governo, volto al raggiungimento degli obiettivi di efficacia ed efficienza della gestione e di buon funzionamento dei controlli interni. Valutare la funzionalità del complessivo sistema dei controlli interni significa favorire la presa di coscienza delle sue componenti da parte delle strutture sottoposte ad auditing e promuovere il raggiungimento delle finalità ad esso connaturate. L'internal auditor è il collante del sistema dei controlli, oltre che il supervisore dei controlli di 1° e 2° livello. Si comprende, quindi, il motivo per cui l'attività di internal auditing viene detta controllo di 3° livello: si tratta di controlli sui controlli e sull'operato delle funzioni che li compongono[84].

Fra le funzioni di controllo quella di revisione interna o Internal audit è certamente la più consolidata nell'ambito del sistema dei controlli interni. L'attività di auditing viene svolta presso organizzazioni che variano per finalità, dimensione, complessità e struttura. La pratica di auditing è, quindi, tanto diffusa, quanto influenzata dalle diversità strutturali, funzionali e giuridiche delle realtà entro le quali vive. Per questo motivo l'IIA (Institute of Internal Auditor) è da anni impegnato nel continuo processo di sviluppo e diffusione di linee guida per l'esercizio dell'attività di revisione interna. L'opera più importante risale al 2004 e contiene gli *Standard for the professional practice of Internal Auditing*[85] che forniscono un framework principle based per lo svolgimento e la promozione dell'attività di Internal audit. L'AIIA (Associazione Italiana di Internal Auditor) rappresenta la sezione italiana dell'IIA e promuove nel nostro paese gli standard, la certificazione, la ricerca e la formazione per la professione di Internal auditor secondo i criteri internazionali.

Il par. 3.4 della Sezione III del Capitolo 7, rubricato "Funzione di revisione interna (internal audit)", stabilisce che la funzione di revisione interna "è volta, da un lato, a controllare, in un'ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi, e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al RAF, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali"[86].

---

[84] Cfr. Dellarosa E., Razzante R., *Il nuovo sistema dei controlli interni della banca*, op. cit., Cap. 9.

[85] Reperibili nella traduzione italiana a cura di AIIA, *Standard internazionali per la pratica professionale dell'Internal Auditing*, Milano, 2006, conforme all'originale IIA, *Standard for the professional practice of Internal Auditing*, Florida, 2004. Ogni due anni gli Standard IIA vengono rivalutati e revisionati alla luce delle evoluzioni in campo professionale e normativo. Le ultime modifiche sono state approvate nel 2012 e sono entrate in vigore il 1° gennaio 2013.

[86] Banca d'Italia, *Circ. n. 263 del 27/12/2006, op. cit., Titolo V,* Capitolo 7, Sezione III, par. 3.4.

Le Disposizioni confermano l'impianto che caratterizza l'Internal audit delle banche e i compiti assegnati alla funzione di revisione interna dalla previgente normativa, ribadendone il consolidato ruolo di controllo di terzi livello[87].

Tuttavia, le Disposizioni prevedono nuove attività di auditing. I previgenti compiti sono, infatti, stati considerevolmente integrati, prevedendo una presenza più significativa ed incisiva su specifici ambiti di intervento, riportati all'interno del Box 11 e approfonditi nel prosieguo del presente paragrafo.

Box 11 - *Gli elementi di novità per l'Internal audit*

La nuova disciplina in materia di revisione interna innova principalmente con riferimento ai seguenti aspetti:

- la verifica sul sistema dei controlli interni;
- la verifica dell'efficacia del RAF e dei pareri preventivi forniti dalla funzione di controllo dei rischi sulle operazioni maggior rilevo;
- la verifica del processo di gestione dei rischi;
- la verifica sulle procedure di continuità operativa;
- il riconoscimento degli Standard Internazionali;
- la collazione organizzativa dell'Internal audit;
- l'attività di reporting dell'Internal audit;
- il follow-up sulle criticità segnalate dal Revisore esterno;
- la redazione del piano di audit pluriennale[88].

In particolare (cfr. Capitolo 7, Sezione III, par. 3.4):

- le Disposizioni affidano alla funzione di revisione interna il compito di sottoporre a verifica di audit il sistema dei controlli interni, nella misura in cui attribuiscono alla stessa il compito di valutare la completezza, l'adeguatezza, la funzionalità, l'affidabilità delle altre componenti del sistema dei controlli interni, del processo di gestione dei rischi e degli altri processi aziendali, avendo riguardo anche alla capacità di individuare errori ed irregolarità, e assegnano alla stessa funzione il compito di sottoporre a verifica le funzioni aziendali di controllo dei rischi e di conformità alle norme;
- all'Internal audit è richiesto di valutare e formulare indicazioni/raccomandazioni sui possibili miglioramenti del sistema dei controlli interni, con particolare riferimento al RAF, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi; una delle novità introdotte dalle Disposizioni riguarda, quindi, il RAF, e in tale ambito, alla funzione di Internal audit spetta il compito di valutare/verificare:
  - l'efficacia del processo di definizione del RAF, la coerenza interna dello schema complessivo e la conformità dell'operatività aziendale al RAF;
  - l'efficacia dei poteri della funzione di controllo dei rischi di fornire pareri preventivi sulla coerenza con il RAF delle operazioni di maggior rilievo;
- con riferimento al processo di gestione dei rischi, la funzione di revisione interna è chiamata a valutare:
  - l'organizzazione, i poteri e le responsabilità della funzione di risk management, anche con riferimento alla qualità e alla adeguatezza delle relative risorse;
  - l'appropriatezza delle ipotesi utilizzate nelle analisi di sensitività e di scenario e negli stress test;
  - l'allineamento con le best practice diffuse nel settore;

[87] Cfr. Quasso F., *L'Internal Audit alla luce delle nuove disposizioni di Vigilanza. Novità ed opportunità*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.
[88] Ibid.

- con riferimento alla continuità operativa, la funzione di revisione interna deve controllare regolarmente il piano aziendale di continuità operativa, prendendo visione dei programmi di verifica, controllandone i risultati e proponendo modifiche al piano sulla base delle mancanze riscontrate; la funzione di revisione interna deve controllare altresì i piani di continuità operativa dei fornitori di servizi e dei fornitori critici.

Altre importanti novità riguardano (cfr. Capitolo 7, Sezione III, par. 3.4):

- l'importante riconoscimento degli Standard Internazionali; le Disposizioni stabiliscono, infatti, che nello svolgimento dei propri compiti la funzione di revisione interna deve tenere conto di quanto previsto dagli standard professionali diffusamente accettati; gli standard a cui si riferisce la previsione normativa sono i sopra citati Standard IIA;
- la collocazione organizzativa dell'Internal audit; le Disposizioni, in merito, collocano la funzione di revisione interna alle dirette dipendenze dell'organo con funzione di supervisione strategica, precisando, tuttavia, che devono essere preservati i raccordi con l'organo con funzione di gestione;
- l'attività di reporting dell'Internal audit nei confronti degli organi aziendali; la previgente disciplina assegnava al responsabile della funzione di revisione interna il compito di informare il C.d.a., il Collegio Sindacale e l'A.d. dell'attività svolta e dei risultati ottenuti; le Disposizioni, invece, precisano che, fermo restando che i destinatari delle comunicazioni delle attività di verifica sono gli organi aziendali e le unità sottoposte a controllo, nella regolamentazione interna deve essere espressamene previsto il potere per la funzione di revisione interna di comunicare in via diretta i risultati degli accertamenti e delle valutazioni agli organi aziendali; gli esiti degli accertamenti che si sono conclusi con giudizi negativi o che evidenziano carenze di rilievo devono essere trasmessi integralmente, tempestivamente e direttamente agli organi aziendali;
- l'attività di follow-up sulle criticità segnalate dal Revisore esterno; in questo ambito la funzione di revisione interna è chiamata a verificare la rimozione delle criticità rilevate dal revisore esterno; le Disposizioni introducono, infatti, due principi riguardanti il rapporto fra l'Internal Audit e il Revisore Esterno, che trovano il proprio fondamento nelle guidance vincolanti dell'IIA; si tratta, in particolare, dello Standard di prestazione 2050 (Coordinamento delle attività) e della Guida Interpretativa Standard 2500 A1-1 (Processo di Follow-Up); lo standard stabilisce che il responsabile internal auditing deve condividere le informazioni e coordinare le diverse attività con i diversi prestatori, esterni e interni, di servizi di assurance e consulenza, al fine di assicurare un'adeguata copertura e minimizzare le possibili duplicazioni; la guida interpretativa stabilisce, invece, che il follow-up sulle azioni intraprese dal management in risposta alle raccomandazioni ricevute deve includere anche quelle avanzate dai revisori esterni.; le Disposizioni, coerentemente con quanto stabilito dall'IIA, impongo all'Internal audit collaborazione e scambio di informazioni con il soggetto incaricato della revisione legale dei conti, e stabiliscono che, nel caso in cui, nell'ambito di questa collaborazione, la funzione di revisione interna venga a conoscenza di criticità emerse durante l'attività di revisione legale dei conti, la stessa debba attivarsi affinché le competenti funzioni aziendali adottino i presidi necessari per superare tali criticità;
- la redazione del piano di audit pluriennale; con riferimento a tale novità, la Banca d'Italia, nell'aggiornamento del 06/06/2014 alla Nota di chiarimenti del 24/01/2014, ha specificato che il piano pluriennale deve essere redatto dalla funzione di revisione interna e approvato dall'organo con funzione di supervisione strategica entro la chiusura dell'esercizio in cui la nuova disciplina è divenuta efficace, ossia entro il 31/12/2014.

Risulta agevole rilevare che, rispetto al passato, è richiesta all'Internal audit una più incisiva e puntuale attività di assurance su diversi temi. Pertanto, è auspicabile che l'Internal audit si faccia parte attiva del processo di cambiamento in corso che interessa il sistema dei

controlli interni, tenendo sempre presente il principio secondo cui il suo operato crea valore se non si limita a individuare le problematiche, ma contribuisce a risolvere[89].

2.2.6 Le novità in materia di outsourcing: graduazione dei requisiti e comunicazioni alla Banca d'Italia

Il ricorso all'esternalizzazione è funzionale ad accrescere la flessibilità organizzativa delle banche che possono così dedicare maggiori risorse al core business oltre che perseguire obiettivi di riduzione dei costi[90].
Ragioni di economicità ed efficienza nello svolgimento dell'attività possono, infatti, condurre in talune ipotesi gli intermediari a privilegiare soluzioni organizzative che prevedano l'esternalizzazione di funzioni. In alcuni casi, l'esternalizzazione può riguardare anche le funzioni di controllo. Nel quadro di una generale disciplina in materia di controlli, si è reso dunque necessario regolare questo aspetto, cercando di contemperare, in generale, esigenze quali la garanzia della predisposizione di strumenti di controllo adeguati, la tutela dell'autonomia delle scelte imprenditoriali, il principio di proporzionalità. Le questioni di maggiore rilevanza attengono, in particolare, ai casi un cui è possibile l'esternalizzazione, alla disciplina delle funzioni di controllo esternalizzate, nonché all'esternalizzazione all'interno dei gruppi bancari[91].

Vale la pena ricordare preliminarmente che la previgente disciplina in materia di esternalizzazione risale alla Circolare n. 229/1999, Titolo IV, Capitolo 11. Tale disciplina, oltre ad avere dimensioni contenute, riguardava unicamente la funzioni di revisione interna. Venivano, inoltre, richiamati in materia di esternalizzazione in ambito bancario i principi contenuti nelle disposizioni del CEBS del dicembre 2006[92].
Con l'intervento di Banca d'Italia del luglio 2013 viene introdotta un'organica disciplina che organizza in modo sistematico le disposizioni in materia di esternalizzazione, creando due regimi diversi e separati a seconda che l'esternalizzazione avvenga nei confronti di una società del gruppo ovvero di un soggetto terzo estraneo allo stesso.

I requisiti richiesti per procedere all'outsourcing al di fuori del gruppo bancario, ossia presso un soggetto esterno alla banca o al suo gruppo, sono graduati in modo diverso a seconda che l'esternalizzazione riguardi funzioni aziendali, funzioni operative importanti e funzioni aziendali di controllo.

Il ricorso all'outsourcing di funzioni aziendali è ammesso a condizione che le banche che ricorrono all'esternalizzazione (cfr. Capitolo 7, Sezione IV, par. 1):
- mantengano il presidio dei rischi derivanti dalle scelte effettuate;
- mantengano la capacità di controllo e la responsabilità sulle attività esternalizzate;
- mantengano le competenze tecniche e gestionali essenziali per re-internalizzare in caso di necessità il loro svolgimento;
- assumano la decisione di ricorrere all'outsourcing coerentemente con la politica aziendale in materia di esternalizzazione, approvata dall'organo con funzione di supervisione strategica.

Vengono, inoltre, espressi alcuni divieti che la banca è chiamata a rispettare nel ricorso all'esternalizzazione. In particolare, la banca non può (cfr. Capitolo 7, Sezione IV, par. 1):
- ¬ delegare le proprie responsabilità, né quella degli organi aziendali;
- ¬ alterare il rapporto e gli obblighi nei confronti dei suoi clienti;

[89] *Ibid*.
[90] Cfr. Banca d'Italia, *Sintesi per gli utenti*, op. cit.
[91] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.
[92] Committee of European Banking Supervisors, *Guidelines on outsourcing*, 14 dicembre 2006.

- pregiudicare il rispetto degli obblighi previsti dalla disciplina di vigilanza, né violare le riserve di attività previste dalla legge;
- pregiudicare la qualità dl sistema dei controlli interni;
- ostacolare la vigilanza.

La novità principale introdotta dalle Disposizioni in materia di esternalizzazioni di funzioni aziendali consiste nell'obbligo per le banche di definire la policy in materia di esternalizzazione[93], il cui contenuto minimo è stabilito dalla nuova disciplina e evidenziato all'interno del Box 12.

Box 12 - *Il contenuto minimo della policy in materia di esternalizzazione*

La politica aziendale in materia di esternalizzazione deve stabilire almeno (cfr. Capitolo 7, Sezione IV, par. 1):
- il processo decisionale per esternalizzare le funzioni aziendali (livelli, funzioni coinvolte, criteri per la scelta e la due diligence del fornitore, valutazione dei rischi, ecc.);
- il contenuto minimo dei contratti di esternalizzazione e i livelli di servizio attesi delle attività esternalizzate;
- le modalità di controllo, nel continuo e con il coinvolgimento della funzione di Internal audit, delle attività esternalizzate;
- i flussi informativi interni rivolti agli organi aziendali e alle funzioni aziendali di controllo, volti ad assicurare la piena conoscenza e governabilità dei fattori di rischio relativi alle funzioni esternalizzate;
- i piani di continuità operativa previsti in caso di non corretto svolgimento delle funzioni esternalizzate da parte del fornitore di servizi (clausole contrattuali, piani operativi, ecc.).

La banca deve, pertanto, verificare l'esistenza della politica aziendale in materia di outsourcing e accertarsi che tale policy disciplini tutti gli aspetti richiamati dalle Disposizioni.

Nel caso di esternalizzazione di funzioni operative importanti[94], di seguito, per semplicità, FOI, la banca deve rispettare condizioni/obblighi che vanno ad aggiungersi a quelli stabiliti per l'esternalizzazione di funzioni aziendali[95].
Le principali novità introdotte in tale ambito sono segnalate all'interno del Box 13.

Box 13 - *I requisiti aggiuntivi per l'esternalizzazione di FOI*

La banca che esternalizza FOI deve altresì (cfr. Capitolo 7, Sezione IV, par. 1):
- conformare il contenuto del contratto ai requisiti previsti dalle Disposizioni; tra questi emergono i livelli di servizio attesi e quelli assicurati in caso di emergenza, le soluzioni di continuità compatibili con le esigenze aziendali, e le modalità di partecipazione alle verifiche dei piani di continuità operativa del fornitore;
- verificare che il fornitore comunichi tempestivamente il verificarsi di incidenti di sicurezza in modo da permettere l'attivazione delle procedure di gestione o emergenza;

[93] Cfr. *Fumagalli M., Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, op. cit.
[94] Per le definizioni di "funzione operativa importante" si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 3.
[95] Per un completo approfondimento delle condizioni da soddisfare nel caso di esternalizzazione di FOI si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione IV, par. 1.

- individuare un referente interno per ciascuna funzione esternalizzata, con il compito di monitorare outsourcer e funzioni,
- acquisire dal fornitore i piani relativi alla continuità operativa;
- garantire il libero accesso a dati e locali del fornitore di servizi da parte della banca, del revisore esterno e delle Autorità di vigilanza[96].

Pertanto, la banca deve verificare il rispetto delle condizioni previste dalla normativa ed eventualmente conformarsi alle stesse.

Per quanto concerne le funzioni aziendali di controllo, le Disposizioni, in linea con il principio di proporzionalità alla base dell'intera disciplina, consentono alle banche di esternalizzare tale categoria di funzioni, stabilendo tuttavia il rispetto, anche in questo caso, di alcuni requisiti aggiuntivi che vanno a cumularsi con quelli richiesti per l'esternalizzazione di funzioni aziendali e di FOI[97].

Tra le ulteriori condizioni che le banche sono chiamate a soddisfare, le novità di maggiore rilievo riguardano il requisito di ammissibilità all'esternalizzazione, la limitazione dei soggetti ai quali è possibile rivolgersi, il contenuto minimo dei contratti e i divieti di incompatibilità del fornitore[98], declinate nei termini riportati all'interno del Box 14.

Box 14 - *Le condizioni per esternalizzare le funzioni aziendali di controllo*

Le Disposizioni ammettono l'esternalizzazione di funzioni di controllo per le sole banche appartenenti, ai fini SREP, alla macro-categoria 4, ed individuano, nelle sole altre banche, associazioni di categoria e società di revisione, i possibili fornitori di servizi. Inoltre sono previsti anche i seguenti ulteriori presidi (cfr. Capitolo 7, Sezione IV, par. 2):

- la previsione di un contenuto minimo aggiuntivo dei contratti di esternalizzazione, rispetto a quello previsto in caso di esternalizzazione di FOI;
- il rispetto da parte del fornitore di servizi del divieto di trovarsi in situazioni di incompatibilità quali, ad esempio, il cumulo di incarichi relativi a funzioni di controllo di 2° e 3° livello per una stessa banca o gruppo, e lo svolgimento della funzione di revisore legale dei conti per la banca che esternalizza o per altre società del gruppo di appartenenza.

Pertanto, qualora la banca non appartenga alla macro-categoria 4, deve procedere con la re-internalizzazione delle funzioni di controllo esternalizzate. La banca deve, inoltre, verificare che il fornitore di servizi scelto per l'esternalizzazione della funzione di controllo rientri tra le tre categorie di soggetti ammessi, che i requisiti aggiuntivi contrattuali previsti dalle Disposizioni siano contenuti nell'accordo di servizio, e che il fornitore non si trovi nelle situazioni di incompatibilità elencate dalla disciplina.

Il par. 3 della sezione in commento prevede numerose novità con riguardo alle comunicazioni da inviare a Banca d'Italia in occasione dell'esternalizzazione di funzioni aziendali. La novità principale riguarda l'obbligo di comunicazione preventiva alla Banca d'Italia dell'intenzione di esternalizzare lo svolgimento, in tutto o in parte, di FOI o di funzioni

[96] Cfr. Fumagalli M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, op. cit.

[97] Per un completo approfondimento delle condizioni da soddisfare nel caso di esternalizzazione di funzioni di controllo si rinvia a Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione II, par. 2.

[98] Cfr. Fumagalli M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, op. cit.

di controllo[99]. Tale comunicazione deve essere inviata almeno 60 giorni prima di conferire l'incarico e deve contenere tutte le indicazioni utili alla verifica del rispetto dei requisiti previsti dalle Disposizioni, e specificare le esigenze che hanno determinato la scelta. La Banca d'Italia, entro 60 giorno dalla ricezione della comunicazione, può avviare un procedimento amministrativo di divieto dell'esternalizzazione, che deve concludersi entro 60 giorni (cfr. Capitolo 7, Sezione IV, par. 3).
Inoltre, entro il 30 aprile di ogni anno, la funzione di revisione interna o il suo referente, se esternalizzata, deve redigere e inviare alla Banca d'Italia una relazione relativa ai controlli svolti sulle funzioni operative importanti o di controllo esternalizzate, alle carenze riscontrate e alle azioni correttive adottate. Tale relazione deve riportare le considerazioni dell'organo con funzione di controllo e essere approvata dall'organo con funzione di supervisione strategica (cfr. Capitolo 7, Sezione IV, par. 3).
Con l'aggiornamento del 06/06/2014 alla Nota di chiarimenti del 24/01/2014, l'Autorità di Vigilanza ha chiarito che la relazione relativa ai controlli svolti sulle attività esternalizzate deve essere redatta e comunicata, per la prima volta, entro il 30/04/2015.

Per quanto concerne, invece, l'esternalizzazione di funzioni aziendali all'interno del gruppo bancario, ossia presso la capogruppo o altra componente del gruppo, le Disposizioni hanno introdotto una disciplina improntata a maggiore flessibilità e con requisiti meno stringenti, in modo da facilitare l'integrazione dei controlli a livello di gruppo anche in considerazione del fatto che il gruppo bancario può essere considerato un unico soggetto economico e che l'esternalizzazione avviene presso società soggette al potere di direzione e coordinamento della capogruppo[100].

Le Disposizioni, infatti, stabilisco che deve valere, per l'intero gruppo bancario, un'unica policy in materia di esternalizzazione che deve essere definita dalla capogruppo e deve avere un contenuto minimo dettagliato dalle Disposizioni (cfr. Capitolo 7, Sezione V, par. 3).
Da segnalare che, rispetto alla policy richiesta in caso di esternalizzazione al di fuori del gruppo bancario, la politica di gruppo deve tenere conto degli interessi degli eventuali soci di minoranza, formalizzando i presidi adottati per assicurare un'adeguata tutela degli stessi.

La maggiore flessibilità che caratterizza la disciplina contenuta nella sezione V, si evince, anche, dal fatto che la stessa stabilisce che il rispetto della politica unica in materia di esternalizzazione da parte della banca appartenente al gruppo, permette alla stessa di derogare alle disposizioni contenute nella Sezione IV (cfr. Capitolo 7, Sezione V, par. 3).
Sono tuttavia, imposti alla banca gli stessi divieti valevoli in caso di esternalizzazione di funzioni aziendali al di fuori del gruppo bancario (cfr. Capitolo 7, Sezione IV, par. 1; Capitolo 7, Sezione V, par. 3).

Nell'aggiornamento del 06/06/2014 alla Nota di Chiarimenti del 24/01/2014, la Banca d'Italia ha ritenuto opportuno ribadire che, in presenza di gruppi bancari, le singole componenti bancarie sono tenute alla definizione della politica aziendale in materia di esternalizzazione verso fornitori di servizi non appartenenti al gruppo, tenuto conto delle disposizioni della capogruppo nell'ambito del potere di direzione e coordinamento. Per le esternalizzazioni all'interno del gruppo, invece, le singole componenti bancarie, ferme restando le responsabilità per le attività esternalizzate, possono non redigere la politica aziendale in materia di esternalizzazione, se adottano e rispettano la politica redatta dalla capogruppo per l'intero gruppo bancario.

[99] *Ibid*.
[100] Cfr. Banca d'Italia, *Sintesi per gli utenti*, op. cit.

Una specifica disciplina è stata, invece, dettata dalla Banca d'Italia in materia di esternalizzazione nell'ambito del gruppo bancario di funzioni aziendali di controllo (cfr. Capitolo 7, Sezione V, par. 3.1).
Nella consapevolezza della necessità di mantenere presidi a tutela del corretto andamento delle società controllate, l'esternalizzazione infragruppo è in generale permessa agli intermediari, indipendentemente dal rispetto del requisito di ammissibilità previsto per l'esternalizzazione al di fuori del gruppo. Le Disposizioni ammettono, infatti, l'esternalizzazione di questa particolare categoria di funzioni presso la capogruppo o le altri componenti del gruppo a prescindere dalle dimensioni e dalla complessità operativa della banca. Tale semplificazione è stata introdotta a motivo della necessità di assicurare l'effettività e l'integrazione dei controlli e, anche, a motivo del fatto che l'esternalizzazione all'esterno del gruppo bancario comporta la dipendenza per lo svolgimento di una determinata attività da un soggetto esterno alla banca o al proprio gruppo, mentre l'esternalizzazione presso la capogruppo o presso atra componente del gruppo costituisce una riallocazione organizzativa dei compiti all'interno di un gruppo sottoposto a direzione e coordinamento unitari.
Tuttavia, al fine di tutelare le società controllate che esternalizzano, fermo restando quanto stabilito dalle disposizioni contenute all'interno del sopra commentato par. 3, il par. 3.1 della sezione in esame impone il rispetto, nel ricorso all'esternalizzazione di funzioni aziendali di controllo all'interno del gruppo bancario, dei seguenti criteri:

- deve essere effettuata e periodicamente aggiornata, in una logica di gruppo, un'analisi dei costi, dei benefici e dei rischi della soluzione adottata dalle banche che hanno optato per l'esternalizzazione di funzioni di controllo;
- gli organi aziendali delle componenti del gruppo devono essere consapevoli delle scelte effettuate dalla capogruppo e sono responsabili dell'attuazione delle strategie e delle politiche perseguite in materia di controlli;
- all'interno delle banche del gruppo e delle altre entità che, secondo la capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso, devono essere nominati appositi referenti, che sono investiti dei seguenti compiti: supportare la funzione aziendale di controllo esternalizzata; riportare alla stessa; segnalare tempestivamente eventi o situazioni suscettibili di modificare i rischi generati dalla banca controllata.

Anche nel caso di esternalizzazione dello svolgimento di FOI o di funzioni di controllo nell'ambito del gruppo di appartenenza, le Disposizioni prevedono l'obbligo per al capogruppo di comunicare preventivamente alla Banca d'Italia l'intenzione delle banche di esternalizzare. Le previsioni relative al contenuto della comunicazione, ai termini di invio della stessa e all'eventuale procedimento amministrativo di divieto dell'esternalizzazione, ricalcano integralmente quanto disposto dalle Disposizioni in caso di esternalizzazione al di fuori del gruppo bancario (cfr. Capitolo 7, Sezione V, par. 4).

Merita osservare che la scelta di dare la possibilità di esternalizzare le funzioni aziendali di controllo, al di fuori del gruppo bancario, alle sole banche appartenenti alla macro-categoria SREP 4 (declinazione del principio di proporzionalità applicabile all'articolazione delle funzioni aziendali di controllo sulla base di criteri quantitativi), e di differenziare la disciplina relativa all'esternalizzazione presso la capogruppo e presso terzi, si contrapponeva al mantenimento dello status quo, ossia:

- principio di proporzionalità non declinato sulla base di criteri quantitativi e conseguente applicazione della disciplina in materia di esternalizzazione tenendo conto della natura, dimensione e complessità dell'attività svolta;
- nessuna differenziazione fra esternalizzazione presso la capogruppo e presso terzi.

Mentre la disciplina posta in consultazione manteneva l'impostazione previgente, ossia non declinava il principio di proporzionalità, limitandosi a circoscrive tale possibilità alle banche di dimensioni contenute o caratterizzate da una limitata complessità operativa, e non distingueva

fra esternalizzazione presso la capogruppo e presso terzi, le Disposizioni, stante le riflessioni condotte alla luce dei risultati della consultazione, concedono, come noto, la possibilità di esternalizzare le funzioni di controllo al di fuori del gruppo bancario alle sole banche appartenenti alla macro-categoria SREP 4 (limitazione che non opera in caso di esternalizzazione di funzioni di controllo infragruppo), e regolano in modo differente l'accentramento presso la capogruppo rispetto a quello al di fuori del gruppo bancario. L'individuazione delle macrocategorie SREP come criterio di ammissibilità, in aggiunta al significativo contenimento dei costi tipico delle operazioni di esternalizzazione, reca il beneficio, della chiarezza, ed è in grado di dar conto delle necessarie esigenze di proporzionalità. La distinzione fra esternalizzazione presso la capogruppo e presso terzi, permette alla prima di contenere i costi a livello consolidato, valorizzando le sinergie informative che si possono cerare a livello di gruppo. I costi legati all'esternalizzazione delle funzioni di controllo, così come configurata dalle Disposizioni, attengono essenzialmente al mantenimento delle competenze necessarie per la re-internalizzazione (obbligo, tra l'altro, non previsto nel caso di esternalizzazione infragruppo) e alla figura del referente per le attività esternalizzate (figura richiesta sia nel caso di esternalizzazione presso la capogruppo, sia presso terzi). Per quanto concerne il sistema economico nel complesso, i costi potrebbero essere legati a possibili distorsioni derivanti dalla sovrapposizione fra i controlli su base consolidata e su base individuale, nel caso in cui questi ultimi siano effettuati a livello di capogruppo. Per quanto riguarda l'autorità, possibili costi potrebbero essere legati all'attivazione di procedimenti amministrativi di divieto dell'esternalizzazione[101].

[101] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.

CAPITOLO 3
La procedura di consultazione e le disposizioni transitorie

3.1 Il resoconto della consultazione: osservazioni e risposte ai quesiti posti dalla Banca d'Italia

Come più volte ricordato nel corso della trattazione dei primi due capitoli, in data 4 settembre 2012 la Banca d'Italia ha posto in consultazione pubblica il documento contenente la proposta della nuova disciplina, rubricato *Documento per la consultazione - Disposizioni di vigilanza prudenziale per le banche - Sistemi dei controlli interni, sistema informativo e continuità operativa*, di seguito, per semplicità, Documento per la consultazione.
La Banca d'Italia, oltre a fornire uno schema delle nuove disposizioni di vigilanza, sollecitava, in generale, commenti sulla proposta di disciplina avanzata, e, in particolare, richiedeva commenti specifici su alcune questioni inserite in appositi quesiti, c.d. boxes.
A consultazione conclusa, la Banca d'Italia ha pubblicato sul proprio sito internet, le osservazioni, i commenti e le proposte pervenute nel corso della consultazione dai rispondenti alla procedura e il resoconto della stessa. Quest'ultimo documento, rubricato *Resoconto della consultazione*, di seguito, per semplicità, Resoconto, sintetizza le risposte ai boxes fornite e riporta, in maniera schematica, le osservazioni formulate dai partecipanti alla consultazione. Ogni osservazione e proposta avanzata è stata attentamente valutata dalla Banca d'Italia, la quale riporta all'interno del Resoconto la propria valutazione. Quest'ultima può essere positiva o negativa o può essersi concretizzata in un chiarimento.
Il presente paragrafo approfondisce le risposte ai quesiti posti dalla Banca d'Italia (par. 3.1.1) e le osservazioni generali avanzate dai rispondenti (par. 3.1.2).

3.1.1 Le risposte ai boxes creati dalla Banca d'Italia

I boxes introdotti dalla Banca d'Italia nel Documento per la consultazione riguardavano i seguenti aspetti (cfr. Documento per la consultazione, Relazione illustrativa, pagg. vii e viii):

- la determinazione della tolleranza al rischio/appetito per il rischio, Box 1;
- l'identificazione delle operazioni di maggior rilievo oggetto del parare preventivo della funzione di controllo dei rischi, Box 2;
- la declinazione del principio di proporzionalità, Box 3;
- l'interazione tra rischio informatico e rischi operativi, Box 4;
- il controllo dei sistemi in cloud computing, Box 5.

Ai fini della nostra analisi analizzeremo nel presente sottoparagrafo le riposte ai primi tre boxes, in quanto concernenti specifici quesiti relativi a particolari disposizioni introdotte in materia di sistema dei controlli interni all'interno del Capitolo 7 del Titolo V della Circolare 263/2006.

Il Documento per la consultazione assegnava all'organo con funzione di supervisione strategica il compito di definire il livello di rischio accettato, facendo coincidere quest'ultimo con la c.d. "tolleranza al rischio" o "appetito per il rischio". Il Box 1 precisava che "la tolleranza al rischio" (risk tolerance) e "l'appetito per il rischio" (risk appetite) sono utilizzati per descrivere sia il livello assoluto di rischio che una banca è a priori disposta ad assumere, sia i limiti effettivi che essa pone nell'ambito di tale livello massimo. Inoltre, sempre all'interno del Box 1, la Banca d'Italia, al fine di valutare l'opportunità di individuare parametri utilizzabili per determinare tale livello di rischio assumibile, sollecitava l'indicazione delle variabili quantitative e qualitative correntemente utilizzate o in via di sviluppo per addivenire a tale determinazione (cfr. Documento per la consultazione, Capitolo 7, Sezione II, par. 2, Box 1).

Il Resoconto evidenzia a tale proposito che:

1. i rispondenti alla consultazione hanno richiesto maggiore chiarezza sulla definizione dei concetti di risk appetite e risk tollerance;
2. i rispondenti hanno proposto due approcci (analitico e sintetico) per la definizione di "appetito per il rischio" e "tolleranza al rischio";
3. è stata sottolineata, da parte delle rispondenti, l'importanza di definire indicatori business-specific e l'inopportunità di utilizzare indicatori quantitativi per i rischi di non conformità, legali e reputazionali;
4. i rispondenti hanno, inoltre, suggerito di definire un contenuto minimale del RAF che preveda obiettivi e limiti almeno in termini di assorbimento di capitale (per i rischi quantificabili) e di liquidità, nonché indicazioni in grado di cogliere l'esposizione ai rischi legali, reputazionali e di compliance;
5. sono stati, infine, proposti elementi qualitativi per i rischi difficilmente misurabili, in particolare di reputazione e di non conformità o per gli statement generali sulle politiche di rischio (ad es. prezzo delle azioni e rating assegnato all'azienda e al suo marchio), e indicatori quantitativi per gli altri rischi (ad es. indicatori di performance e di rischio).

Come noto, l'esigenza di cui al punto 1 è stata condivisa dalla Banca d'Italia, la quale ha, infatti, modificato le previsioni disciplinari proposte, introducendo le definizioni di RAF, risk capacity, risk appetite, risk tolerance, risk profile e risk limits viste all'interno del paragrafo 2.2.1.

In merito, invece, alla definizione di "appetito per il rischio" e di "tolleranza al rischio" sono stati proposti, come anticipato al punto 2, due diversi approcci:

- l'approccio analitico, che presuppone la definizione di un panel di indicatori quali-quantitavi di appetito/tolleranza al rischio distinti per le diverse tipologie di rischio;
- l'approccio sintetico, che presuppone la creazione di un unico indice di rischio basato sulla combinazione di indicatori di natura diversa normalizzati e ponderati; tale indice unico presenta lo svantaggio di essere difficilmente interpretabile, in quanto costituito da indicatori relativi a singoli segmenti di rischio non necessariamente omogenei.

In entrambi gli approcci, gli indicatori quantitativi indicati dai rispondenti alla procedura di consultazione includono misure di capitale economico, requisiti patrimoniali ed elementi di stato patrimoniale, mentre gli indicatori qualitativi individuati sono il rating obiettivo della banca e gli statement sui fattori di rischio che la banca non ha intenzione di assumere o che vuole contenere. I rispondenti hanno inoltre proposto, per le banche di minori dimensioni e complessità operativa, coerentemente con il principio di proporzionalità, l'individuazione di parametri più comunemente utilizzati nella prassi aziendale, quali: Core Tier 1 (CT1), Total Capital Ratio (TCR) ovvero indicatori analoghi che tengano conto anche dei rischi di secondo pilastro.

Dalle risposte pervenute emerge, tuttavia, un quadro di grande eterogeneità di approcci: se per molti intermediari la formalizzazione del RAF tende a coincidere con il processo ICCAP, altri fanno riferimento a misure di volatilità, profitti, capitale a rischio, liquidità e rating obiettivo. È emerso, inoltre, che in alcuni casi nel RAF vengono esplicitati elementi qualitativi quali: la diversificazione delle fonti di liquidità, il rischio legale e reputazionale e il rischio di compliance regolamentare[102].

La Banca d'Italia nel Resoconto, per quanto concerne i commenti e le proposte avanzate, ha affermato che fornire puntuali indicazioni sui parametri da utilizzare sarebbe stato inopportuno, dato che ne sarebbero derivati vincoli troppo onerosi, in caso di ampie e sofisticate definizioni, ovvero rischi di appiattimento, in caso di definizioni standard e semplificate. A tale proposito, la Banca d'Italia sostiene che il necessario utilizzo di metriche quantitative ma anche di indicazioni qualitative deve fare i conti con l'utilizzo di prassi

[102] Cfr. Banca d'Italia, *Relazione sull'analisi d'impatto*, op. cit.

aziendali molto eterogenee: esse scontano le notevoli differenze esistenti nei sistemi di definizione e misurazione dei rischi, diretta conseguenza anche delle caratteristiche dimensionali e operative.
Ciò premesso, la Banca d'Italia ha preferito enunciare all'interno del Resoconto alcuni principi cui informare la struttura del RAF. Tali principi si riferiscono al contenuto minimale del RAF e all'utilizzo di parametri quantitativi e qualitativi, e sono stati inseriti dalla Banca d'Italia all'interno della disciplina contenuta nell'Allegato C alle Disposizioni, già affrontata all'interno del paragrafo 2.2.1.

All'interno del Box 2, la Banca d'Italia, sollecitava commenti volti ad individuare criteri qualitativi e quantitativi sulla base dei quali l'organo con funzione di supervisione strategica doveva definire i criteri per individuare le operazioni di maggior rilievo da sottoporre al vaglio preventivo della funzione di controllo dei rischi, di seguito, per semplicità, OMR (cfr. Documento per la consultazione, Capitolo 7, Sezione II, par. 2, Box 2).
Con riferimento al box in esame, Il Resoconto riporta i seguenti commenti avanzati dai rispondenti alla consultazione:

1. è stato proposto di non rendere il parere della funzione di risk management ridondante rispetto a quello formulato dai soggetti che propongono l'assunzione del rischio; esso potrebbe riguardare una valutazione circa la potenziale redditività dell'operazione ma non dovrebbe riguardare aspetti di competenza di altre funzioni; in altre parole, il potere della risk management function di pronunciarsi preventivamente sulla coerenza delle OMR con la politica di governo dei rischi dovrebbe arricchire la prospettiva di giudizio promuovendo una visione olistica e non focalizzandosi su un singolo rischio;
2. per identificare le OMR sono stati proposti, tra gli altri, due criteri: l'apporto marginale che l'operazione potrebbe produrre in termini di assorbimento del livello di risk tollerance prescelto, e la percentuale di assorbimento di capitale interno e di capitale interno complessivo che l'operazione potrebbe determinare;
3. è stato inoltre suggerito di identificare le OMR con le operazioni che modificano l'operatività della banca, quali: le operazioni di intermediazione o investimento che modificano l'equilibrio economico/patrimoniale, misurato secondo logiche ICAAP; le operazioni straordinarie, cessioni/aperture di sportelli e aperture di sedi distaccate; i contratti di outsourcing, le operazioni di re-internalizzazione e le scelte in materia di continuità operativa; le deroghe a parametri qualitativi previsti nelle singole policy;
4. infine, sono stati suggeriti ulteriori criteri per individuare le OMR, come le caratteristiche della controparte (ad es. sede in giurisdizioni "non trasparenti" e/o struttura societaria complessa), la tipologia dell'operazione (ossia operazioni che implicano specifiche deroghe a standard operativi e contrattuali, ad es. operazioni di investimento attraverso il ricorso a special purpose vehicles o altre strutture complesse), la coerenza con gli indirizzi strategici e la non ricorrenza di operazioni significative per dimensione e complessità (ad es. lunga scadenza, remunerazione articolata e struttura delle garanzie complessa).

Nonostante alcuni rispondenti alla consultazione abbiamo identificato i criteri di cui sopra, in via generale, è stata fatta richiesta di riconoscere autonomia all'organo con funzione di supervisione strategica, in quanto la prescrittività sull'argomento potrebbe esporre a rischi, quali mancanza di uniformità e inclusione nella definizione di alcune operazioni e non di altre[103].
Con riferimento all'osservazione di cui al punto 1, la Banca d'Italia nel Resoconto ha precisato che le OMR non devono ricadere nella competenza diretta degli organi aziendale.
Tale precisazione è stata ulteriormente fornita dalla stessa Autorità con l'aggiornamento del 06/06/2014 alla Nota di chiarimenti del 24/01/2014, nell'ambito del quale è stato specificato

[103] *Ibid*.

che l'obbligo non riguarda le OMR che rientrano nella diretta competenza degli organi di supervisione strategica e di gestione, ancorché la richiesta in tali circostanze di pareri consultivi al risk management può rappresentare una buona prassi gestionale.
Per quanto concerne i criteri da individuare per identificare le OMR, la Banca d'Italia ha affermato che questi devono essere coerenti con il RAF e idonei a censire le operazioni nel caso vi siano potenziali conflitti di interesse. La Banca d'Italia, quindi, lascia autonomia agli intermediari nella valutazione della rilevanza di un'operazione, nel rispetto, tuttavia, dei due requisiti suddetti. Pertanto, la proposta di disciplina e le Disposizioni accolgono la sub-opzione regolamentare secondo cui le ORM sono definite dagli intermediari che valutano con autonomia la rilevanza di un'operazione[104].

La bozza di disciplina sollecitava commenti per declinare nel concreto la possibilità concessa alle banche di accorpare ovvero esternalizzare le funzioni aziendali di controllo, sulla base di criteri riferiti alla dimensione e alla complessità operativa, nonché avuto riguardo all'esigenza di assicurare un rapporto ottimale costi-benefici nell'articolazione e nella conduzione dei controlli (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 1, Box 3).
Il Resoconto evidenzia che sono stati suggeriti dai rispondenti vari criteri per declinare il principio di proporzionalità con riferimento all'esternalizzazione delle funzioni aziendali di controllo, tra cui: la quotazione dell'intermediario, la tipologia di attività svolta, la dimensione del portafoglio gestito, l'utilizzo di sistemi interni di misurazione dei rischi, la macro-categoria SREP di appartenenza.
Con riferimento a tali criteri, la Banca d'Italia ha accolto, come noto, il criterio dell'appartenenza alle macrocategorie SREP e ha declinato in termini puntuali tale principio con riferimento all'esternalizzazione al di fuori del gruppo bancario delle sole funzioni aziendali di controllo e non anche con riguardo alle FOI.
Nell'ambito della consultazione, inoltre, un numero consistente di rispondenti ha sollevato critiche nei confronti della proposta di disciplina con riferimento:

1. alla mancata distinzione fra esternalizzazione presso la capogruppo o verso il network (BCC), e presso terzi (cfr. Documento per la consultazione, Capitolo 7, Sezione IV);
2. alla norma che prevede di mantenere le competenze per l'eventuale re-internalizzazione, da cui deriverebbero, soprattutto secondo gli intermediari più piccoli, costi troppo elevati che priverebbero di convenienza economica la soluzione adottata (cfr. Documento per la consultazione, Capitolo 7, Sezione IV, par. 1);
3. alla mancanza di flessibilità organizzativa rispetto alle soluzioni volte a controllare le attività esternalizzate; a tale proposito, la proposta di disciplina disponeva l'obbligo di individuare un responsabile del controllo delle singole funzioni esternalizzate dotato di adeguati requisiti di professionalità, c.d. referente per le attività esternalizzate (cfr. Documento per la consultazione, Capitolo 7, Sezione IV, par. 1).

La critica di cui al punto 1 ha determinato la differenziazione della disciplina dell'esternalizzazione all'esterno del gruppo bancario di appartenenza da quella dell'esternalizzazione presso la capogruppo o altra componente del gruppo.
Con riferimento, invece, alla critica di cui al punto 2, le Disposizioni hanno mantenuto l'obbligo per le banche di conservare le competenze necessarie per l'eventuale re-internalizzazione delle funzioni di controllo esternalizzate, non estendendo, tuttavia, tale norma al caso dell'esternalizzazione infragruppo.
È rimasta ferma, inoltre, la norma che dispone l'obbligo a carico delle banche di individuare, all'interno della propria organizzazione, un referente per le attività esternalizzate.

[104] Vedi infra par. 2.2.4.

3.1.2 Le osservazioni alla proposta di disciplina

I rispondenti alla procedura di consultazione hanno avanzato commenti, richieste di modifiche e di chiarimenti su argomenti specifici trattati dalla proposta di disciplina. Come già accennato all'interno del paragrafo 3.1, il Resoconto della Banca d'Italia, oltre ad aver sintetizzato le risposte ai boxes fornite dai rispondenti, ha riportato, in modo schematico, le principali osservazioni alla bozza di disciplina e le correlate valutazioni della Banca d'Italia.
Il presente paragrafo si pone l'obiettivo di informare sulle osservazioni maggiormente significative avanzate dai rispondenti, che, in taluni casi, hanno determinato la modifica del testo normativo.

Con riferimento alla Sezione I del Capitolo 7, rubricata "Disposizioni preliminari e principi generali", le principali osservazioni avanzate riguardano i seguenti aspetti:
- l'inquadramento della funzione antiriciclaggio;
- la verifica del grado di aderenza ai principi del sistema dei controlli interni;
- il processo di valutazione delle attività aziendali;
- la mappatura dei rischi.

La proposta di disciplina non menzionava mai la funzione antiriciclaggio. Pertanto, i rispondenti hanno chiesto alla Banca d'Italia di chiarire se il Capitolo 7 dovesse applicarsi anche a tale funzione, almeno nelle sue parti generali e non diversamente disciplinate, o se questa rimanesse regolata esclusivamente dal provvedimento specifico del marzo 2011[105], anche qualora i compiti di antiriciclaggio fossero stati assegnati dalla nuova disciplina alla compliance o al risk management. La Banca d'Italia ha, a tale proposito, chiarito che la nuova disciplina si applica anche alla funzione antiriciclaggio per le parti non diversamente disciplinate da quest'ultimo provvedimento.

Con riferimento all'ultimo capoverso della Sezione I, il quale imponeva alla banche di verificare, almeno annualmente, il grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione e di adottare le misure adeguate per rimediare a eventuali carenze riscontrate (cfr. Documento per la consultazione, Capitolo 7, Sezione I, par. 6), i rispondenti alla consultazione hanno chiesto di chiarire:
a) se fosse sufficiente una delibera di valutazione dei risultati delle relazioni delle funzioni di controllo corredata delle relative considerazioni dell'organo con funzione di supervisione strategica;
b) se la valutazione dovesse essere svolta dall'organo con funzione di supervisione strategica sentito l'organo con funzione di controllo.

La Banca d'Italia, al riguardo, ha chiarito che la delibera di cui al punto a) rappresenta l'attività di verifica minimale che le banche devono svolgere. La Banca d'Italia ha specificato, infatti, che l'attività di verifica di cui all'ultimo capoverso della Sezione I deve avere frequenza maggiore ed essere innescata da flussi informativi diversi dalle relazioni delle funzioni di controllo: in generale, qualsiasi evento astrattamente idoneo a evidenziare carenze nel sistema dei controlli interni deve essere portato a conoscenza degli organi aziendali, che devono verificare la gravità della carenza e porre in essere i rimedi necessari a rimuoverla.
L'aggiornamento della Banca d'Italia del 06/06/2014 alla Nota di chiarimenti del 24/01/2014 ha aggiunto, a tale proposito, che la verifica del grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione, assegnata genericamente alle banche, ancorché sembrerebbe coincidere con la verifica periodica sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni che deve essere svolta dalla funzione di revisione

[105] Banca d'Italia, *Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art. 7 comma 2 del Decreto Legislativo 21 novembre 2007, n. 231*, 10 marzo 2011.

interna, è rimessa alla responsabilità degli organi aziendali, ciascuno secondo le proprie competenze.

Per quanto concerne il processo di valutazione delle attività aziendali, il Documento per la consultazione prevedeva la formalizzazione dei processi e delle metodologie di valutazione, anche a fini contabili, delle attività aziendali e la verifica della loro affidabilità e integrazione con il processo di gestione dei rischi (cfr. Documento per la consultazione, Capitolo 7, Sezione I, par. 6).
È stato chiesto, in merito, di:

a) definire il significato di attività aziendali;
b) chiarire le modalità di integrazione dei processi e delle metodologie di valutazione con quelli di risk management;
c) limitare la portata della norma alle sole attività complesse;
d) indicare quali fossero gli altri fini, oltre a quelli contabili, per cui tali processi dovevano essere utilizzati.

La Banca d'Italia, in relazione ai chiarimenti richiesti, ha fatto presente che per attività aziendali si intendono tutti gli elementi che costituiscono l'attivo della banca on-balance e off-balance, e che l'integrazione con il processo di risk management è cruciale in quanto questo riguarda in modo trasversale tutta l'operatività aziendale e non è limitato alla sola funzione di controllo dei rischi. L'integrazione, ha specificato la Banca d'Italia all'interno del Resoconto, deve ad esempio consentire di riconciliare le valutazioni contabili con quelle effettuate a fini di controllo del rischi o a fini operativi/gestionali. A tale scopo i dati e i modelli utilizzati per i vari fini devono essere affidabili e tra loro raccordabili. Tra le finalità per cui tali processi possono essere utilizzati, la Banca d'Italia ha menzionato, a titolo esemplificativo, fini di risk management o gestionali. In merito, invece, alla portata della norma, la Banca d'Italia ha chiarito che deve essere applicata a tutte le attività e ha specificato che, per le attività complesse, per le quali più frequente è l'utilizzo di modelli e di valutazioni interne, la verifica dell'affidabilità deve essere effettuata con particolare cura e attenzione.
Importanti chiarimenti sono stati forniti dall'Autorità anche nell'ambito dell'aggiornamento del 06/06/2014 alla Nota del 24/01/2014. La Banca d'Italia ha ricordato che l'errata valutazione delle attività aziendali a causa dell'implementazione di processi e metodologie non affidabili e/o non integrati con il processo di gestione dei rischi può impattare su diverse tipologie di rischio (finanziari, legali, operativi e reputazionali). Per quanto concerne le metriche attraverso cui valutare il rischio di non corretta valutazione delle attività aziendali, la definizione e lo sviluppo delle stesse sono rimessi all'autonomia organizzativa delle banche.

Infine, per quanto riguarda la mappatura dei rischi, i rispondenti hanno chiesto se fosse necessario procedere alla formalizzazione della stessa per renderla disponibile alle varie strutture e quale dovesse essere il relativo livello di analiticità. Inoltre, è stata chiesta la possibilità di sviluppare un'unica fase di identificazione dei rischi comune per le funzioni di controllo di 2° e 3° livello.
La Banca d'Italia ha chiarito la necessità che l'organo con funzione di supervisione strategica formalizzi e comunichi alle strutture/funzioni interessate la mappatura dei rischi assunti dalla banca, con evidenza dei rischi cui sono esposte le varie unità operative. Mentre, per quanto concerne il livello di analiticità della mappature ha specificato che lo stesso deve essere coerente con il principio di proporzionalità e dunque riflettere le dimensioni e la complessità operativa della banca. La richiesta di implementare un fase di identificazione dei rischi unica per tutte le funzioni aziendali di controllo è stata, invece, accolta dalla Banca d'Italia.

Con riferimento alla Sezione II del Capitolo 7, rubricata "Il ruolo degli organi aziendali", le principali osservazioni avanzate riguardano:

- la gestione integrata dei rischi;
- il rapporto tra l'organo con funzione di controllo e l'O.d.V. ex d.lgs. 231/2001.

Nel primo capoverso del paragrafo 3, dedicato all'organo con funzione di gestione, il Documento per la consultazione inseriva la locuzione "gestione integrata" (cfr. Documento per la consultazione, Capitolo 7, Sezione II, par. 3).
I rispondenti hanno chiesto alla Banca d'Italia di precisare meglio il significato di tale locuzione in relazione con il principio di proporzionalità. Ad esempio è stato chiesto di chiarire se l'approccio building block, utilizzato per la determinazione del capitale interno complessivo e che esclude le correlazioni tra i rischi, possa essere considerato coerente con la gestione integrata dei rischi richiesta.
La Banca d'Italia, per quanto concerne l'osservazione di cui sopra, ha chiarito che:

- la gestione integrata dei rischi attiene in primo luogo a profili di natura gestionale e organizzativa; nel momento in cui la banca assume, in linea con i propri obiettivi, un determinato rischio deve valutare gli effetti che tale assunzione ha sugli altri rischi e rafforzare, ove necessario, i presidi organizzativi e patrimoniali;
- quanto agli aspetti relativi alla quantificazione del capitale, nel processo di aggregazione dei rischi le banche devono identificare e valutare gli effetti delle concentrazioni che possono emergere dall'interazione tra i diversi rischi, soprattutto in condizioni di stress;
- in applicazione del principio di proporzionalità, le banche di minore dimensione e complessità possono limitarsi a sommare il capitale interno calcolato a fronte dei singoli rischi e a valutare le interazioni tra i rischi adottando un approccio qualitativo e semplificato.

In merito al rapporto tra l'organo con funzione di controllo e l'O.d.V., la proposta di disciplina disponeva l'obbligo per il primo di svolgere le funzioni dell'Organismo di Vigilanza, con possibilità di scelta difforme, ossia affidare tali funzioni a un organismo appositamente istituito, al ricorrere di particolari e motivate esigenze (cfr. Documento per la consultazione, Capitolo 7, Sezione II, par. 4).
Considerata la ristrettezza delle circostanze nelle quali la banca può optare per la separatezza, la coincidenza diveniva essenzialmente l'unica scelta. Pertanto, è stato chiesto di riformulare tale disposizione, nel senso di riconoscere maggiore flessibilità alla banca nell'assegnare tali funzioni a un organismo appositamente istituito.
La Banca d'Italia, al fine di tener conto delle esigenze di flessibilità organizzativa ricordate dai rispondenti, ha modificato la previsione normativa, sottolineando, come noto, il carattere derogabile della disposizione, non solo al ricorrere di particolari esigenze, ma ogniqualvolta la banca sia in grado di motivare la scelta del regime derogatorio.

All'interno dell'ultimo paragrafo della Sezione II, dedicato al tema del coordinamento tra funzioni e organi di controllo, l'Autorità di vigilanza affidava all'organo con funzione di supervisione strategica il compito di approvare un documento di coordinamento dei vari organi e funzioni di controllo al fine di assicurare una corretta interazione tra le strutture con compiti di controllo e evitare sovrapposizioni o lacune (cfr. Documento per la consultazione, Capitolo 7, Sezione II, par. 5).
Con riguardo a tale documento, i rispondenti hanno chiesto di rivedere il processo di approvazione proposto dalla disciplina, considerato che, in alcuni casi, l'organo con funzione di supervisione strategica si troverebbe costretto ad approvare due volte gli stessi contenuti. Gli stessi rispondenti hanno, inoltre, proposto di affidare alle strutture interessate, con il coinvolgimento dell'organo con funzione di gestione, lo svolgimento della fase di analisi dell'andamento dei flussi informativi e delle aree di sovrapposizione e sinergia, ferma restando la reportistica all'organo con funzione di supervisione strategica.
La Banca d'Italia ha confermato che l'approvazione del documento di coordinamento deve essere di competenza dell'organo con funzione di supervisione strategica, atteso il suo carattere strategico per il corretto funzionamento del sistema dei controlli interni, accogliendo, però, la proposta avanzata dai rispondenti. L'Autorità ha, infatti, chiarito che l'analisi

preliminare dei flussi informativi e l'individuazione delle aree di sovrapposizione sulla base della quale redigere il documento può essere condotta dall'organo con funzione di gestione con il coinvolgimento delle strutture interessate.

Con riferimento alla Sezione III del Capitolo 7, rubricata "Funzioni aziendali di controllo", le principali osservazioni avanzate riguardano i seguenti aspetti:

- la nomina dei responsabili delle funzioni aziendali di controllo;
- l'amministratore delegato con responsabilità di funzioni di controllo;
- il programma di attività delle funzioni di controllo di 2° livello;
- gli oneri di rendicontazione a carico delle funzioni aziendali di controllo.

In merito alla figura del responsabile di ciascuna funzione aziendali di controllo, il Documento per la consultazione assegnava all'organo con funzione di gestione il compito di provvedere alla sua nomina/revoca (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 1).
In proposito, è stato chiesto di chiarire se tale previsione fosse in contrasto con quella sulla non delegabilità all'organo con funzione di gestione del potere di nomina del responsabile delle funzioni di revisione interna e di conformità prevista dal provvedimento della Banca d'Italia sul governo societario[106]. È stato chiesto, quindi, di prevedere che la nomina dei responsabili fosse deliberata dall'organo con funzione di supervisione strategica, previo parere dell'organo di controllo. La Banca d'Italia ha accolto la richiesta, modificando nei termini suggeriti il testo normativo.

La proposta di disciplina disponeva, inoltre, che il responsabile di ciascuna funzione aziendale di controllo poteva essere un componente dell'organo amministrativo, purché non destinatario di altre deleghe operative (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 1).
I rispondenti hanno chiesto di temperare il divieto di attribuire la responsabilità di una funzione di aziendale di controllo a un amministratore titolare di deleghe operative in funzione del principio di proporzionalità.
La Banca d'Italia ha chiarito che, in generale, i responsabili delle funzioni aziendali di controllo non possono avere la titolarità di aree operative sottoposte al proprio controllo, mentre la possibilità di affidare agli stessi aree operative non sottoposte al loro controllo va attentamente valutata alla luce dei principi generali di prevenzione dei conflitti di interesse ed efficacia/efficienza operativa. La Banca d'Italia, sulla base di tali principi, ha, pertanto, chiarito che un amministratore potrebbe essere responsabile di una funzione aziendale di controllo e al contempo di deleghe operative solo se queste non riguardano attività sottoposte al suo controllo o possono creare conflitti di interessi.

Per quanto concerne l'obbligo, a carico delle funzioni di controllo di 2° livello, di presentare annualmente agli organi aziendali un programma delle attività di controllo da porre in essere (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 2), i rispondenti alla procedura di consultazione hanno chiesto di precisare i criteri da seguire per identificare il contenuto dello stesso.
La Banca d'Italia, in merito, non ha chiarito quale sia il contenuto del programma, limitandosi a precisare che lo stesso deve soddisfare la finalità di fissare le priorità tra le attività da svolgere e rappresentare ai vertici gli aspetti di maggior rilievo che impegneranno la funzione che lo ha redatto.

Infine, relativamente agli oneri di rendicontazione, le funzioni aziendali di controllo erano obbligate a riferire in merito alla completezza, adeguatezza ed affidabilità del sistema

[106] Cfr. Banca d'Italia, *Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, op. cit., par. 2.1, Linee applicative, lettera b).

dei controlli interni e a presentare agli organi aziendali una relazione sull'attività svolta e un programma di attività (piano di audit per la funzione di revisione interna) (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 2).
È stato chiesto, in merito, di semplificare e ridurre le richieste di rendicontazione riferite a intermediari di dimensione contenuta o contrassegnati da limitata complessità operativa e bassa propensione al rischio.
La Banca d'Italia ha espresso una valutazione negativa. Pertanto, l'obbligo di rendicontazione non è venuto meno, né è stato ridimensionato in funzione dei parametri suggeriti. La Banca d'Italia ha fatto presente, però, che l'entità della rendicontazione richiesta per assolvere agli obblighi imposti è essa stessa connessa alla dimensione e al grado di complessità operativa di ogni banca.

Con riferimento al paragrafo 3.2 della Sezione III, dedicato alla funzione di conformità alle norme (compliance), la principale osservazione avanzata riguarda il perimetro di competenza della funzione di compliance.
La proposta di disciplina prevedeva la gestione da parte della stessa funzione del rischio di non conformità alle norme con riguardo a tutta l'attività aziendale, specificando che particolare attenzione doveva essere posta anche nella verifica della conformità alle normative di natura fiscale e del coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 3.2).
In materia, i rispondenti hanno richiesto di chiarire:

a) come debba essere interpretata la frase "presiede alla gestione del rischio di non conformità […] con riguardo a tutta l'attività aziendale", contenuta nella proposta di disciplina; se tale locuzione doveva essere intesa nel senso di prevedere una responsabilità ultima della funzione di conformità per tutte le normative che hanno impatto aziendale, i rispondenti hanno osservato che non sarebbe stato operativamente praticabile in molte realtà, soprattutto di minori dimensioni, ed è spesso in contrasto con il principio di economicità;
b) il perimetro di competenza e la responsabilità della funzione di compliance per quelle normative che non regolano o non sono direttamente attinenti allo svolgimento dell'attività bancaria, per le quali la normativa settoriale prevede la presenza di specifiche figure di riferimento e garanzia (ad es., normativa privacy, responsabile della sicurezza);
c) la previsione secondo la quale le banche dovevano tener conto dei rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

Come adeguatamente segnalato all'interno del paragrafo 2.2.3, la Banca d'Italia ha modificato le previsioni in parola introducendo il principio secondo cui, ferma restando l'estensione del rischio di non conformità presidiato dalla compliance a tutte le disposizioni applicabili alle banche, il coinvolgimento della funzione deve essere proporzionale al rilievo che le singole norme hanno per l'attività svolta e alle conseguenze della loro violazione. Pertanto, l'Autorità di vigilanza ha disposto il coinvolgimento massimo della funzione per l'attività di prevenzione e gestione del rischio di violare le norme per le quali non siano previste forme di presidio specializzato e le norme più rilevanti, mentre, in relazione ad altre normative per le quali siano già previste forme specifiche di presidio specializzato all'interno della banca, ha stabilito che il coinvolgimento della funzione di compliance può essere meno intenso ma mai assente. Con riferimento alle norme tributarie, la Banca d'Italia ha disposto, invece, che il ruolo della compliance può limitarsi alla definizione di procedure che, per quanto possibile, pongano la banca al riparo dalle conseguenze, sia sanzionatorie sia reputazionali, di una loro violazione.
Per quanto concerne, invece, il compimento di operazioni per conto della clientela in violazione/elusione di norme fiscali, la Banca d'Italia ha chiarito che ciò espone la banca a rilevanti rischi, anche di natura reputazionale e, pertanto, la banca deve adottare ogni tutela

per evitare di essere coinvolta in operazioni di tale natura, anche tenuto conto del livello di diligenza professionale cui è tenuta.

Con riferimento al paragrafo 3.3 della Sezione III, dedicato alla funzione di controllo dei rischi (risk management function), le principali osservazioni avanzate riguardano:

- la collocazione del CRO (Chief Risk Officer);
- il parere sulle OMR;
- gli indicatori di anomalia o inefficienza dei sistemi di misurazione e controllo dei rischi.

Relativamente alla prima osservazione, i rispondenti alla consultazione hanno chiesto di riconoscere la possibilità che venga istituita una figura di supervisione e coordinamento di autonome e separate funzioni aziendali (c.d. CRO).
È stato, altresì, richiesto di riconoscere esplicitamente la possibilità che al CRO riportino gerarchicamente sia il responsabile della funzione di risk management, sia quello della funzione di compliance e ciò in quanto:

a) favorirebbe un approccio maggiormente integrato alla gestione dei rischi;
b) vi sarebbero strette relazioni tra il potere di fornire pareri preventivi del risk management e le valutazioni ex-ante tipicamente effettuate dalla compliance;
c) si garantirebbe una maggiore flessibilità organizzativa.

Relativamente alle richieste di cui sopra, la Banca d'Italia ha espresso contrarietà all'istituzione della figura del CRO cui riportino gerarchicamente i responsabili delle funzioni di 2° livello e ha osservato che:

- in linea con quanto stabilito dalle linee guida internazionali[107], il CRO è il responsabile della funzione di risk management e, in quanto tale, non può essere sovraordinato gerarchicamente al responsabile della funzione di compliance; le due funzioni, infatti, essendo entrambe di 2° livello e richiedendo professionalità tra loro eterogenee, sebbene complementari, devono conservare una certa indipendenza reciproca e autonomia di giudizio;
- l'istituzione di una figura di coordinamento dei controlli di 2° livello, cui riportano gerarchicamente i responsabili delle funzioni di 2° livello, non è compatibile con l'assetto del sistema dei controlli interni e provocherebbe la creazione di un ulteriore livello tra le funzioni di 2° livello e l'organo con funzione di gestione cui queste riportano gerarchicamente, con il rischio che la loro dialettica diretta venga filtrata dal soggetto intermedio.

La Banca d'Italia ha specificato, tuttavia, che all'interno dell'organo con funzione di gestione o dell'organo con funzione di supervisione strategica può essere specificatamente individuato un amministratore che assuma il ruolo di coordinamento delle funzioni aziendali di controllo.

Con riguardo al compito assegnato alla funzione di controllo dei rischi di esprimere pareri preventivi sulla coerenza con la politica di governo dei rischi delle OMR (cfr. Documento per la consultazione, Capitolo 7, Sezione III. par. 3.3), è stato chiesto di integrare la previsione inserendo il periodo finale secondo cui la stessa funzione, nell'esprime i suddetti pareri, può acquisire quelli di altre funzioni interne coinvolte nel processo di gestione dei rischi (ad. es. funzione di compliance, funzione ICT).
Inoltre, è stato chiesto di valutare una proposta alternativa di previsione normativa secondo cui il risk management verificherebbe ex-post, e non ex-ante, le OMR.
La Banca d'Italia ha accolto positivamente la richiesta di integrazione della previsione normativa e ha ampliato quest'ultima con il seguente inciso: "eventualmente acquisendo, in funzione della natura dell'operazione, il parere di altre funzioni coinvolte nel processo di gestione dei rischi"[108].

[107] Cfr., tra l'altro, EBA, *Guidelines on Internal Governance*, op. cit., e FSB, *Thematic Review on Risk Governance*, op. cit.
[108] Cfr. Banca d'Italia, *Circ. n. 263 del 27/12/2006,* op. cit., Titolo V, Capitolo 7, Sezione III, par. 3.3.

In relazione all'ulteriore richiesta avanzata, la Banca d'Italia ha ritenuto opportuno chiarire che il parere preventivo è una misura di escalation volta a coinvolgere gli organi aziendali su determinate operazioni, normalmente di competenza delle funzioni di business che, per i particolari profili di rischio, sono ritenute dal risk management meritevoli di particolare attenzione.

Il Documento per la consultazione inseriva nel novero delle attribuzioni alla risk management function anche il compito di sviluppare e applicare indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi, c.d. indicatori di anomalia o inefficienza (cfr. Documento per la consultazione, Capitolo 7, Sezione III, par. 3.3). I rispondenti alla consultazione hanno chiesto di eliminare tale compito.
La Banca d'Italia si è espressa in senso negativo e ha specificato che lo sviluppo di tali indicatori è da ritenersi opportuno al fine di verificare nel continuo l'affidabilità dei sistemi di misurazione e controllo dei rischi impiegati.

Con riferimento al paragrafo 3.4 della Sezione III, dedicato alla funzione di revisione interna (internal audit), la principale osservazione avanzata riguarda l'applicazione degli Standard Internazionali di Internal audit. È stato suggerito di prevedere un richiamo all'opportunità di rifarsi agli stessi, anche sulla base di quanto espresso nel documento *The internal audit function in banks* del Comitato di Basilea del giugno 2008.
La Banca d'Italia ha accolto positivamente tale osservazione e ha inserito all'interno del paragrafo in esame la previsione normativa secondo cui, nello svolgimento dei propri compiti, la funzione di revisione interna deve tenere conto di quanto previsto dagli standard professionali diffusamente accettati.

I rispondenti hanno, inoltre, criticato alcuni aspetti inerenti la disciplina contenuta all'interno della Sezione IV del Capitolo 7, rubricata "Esternalizzazione di funzioni aziendali (outsourcing)". Le principali osservazioni avanzate in materia riguardano:
- la limitazione del novero dei soggetti presso cui esternalizzare le funzioni di controllo;
- l'obbligo di informativa preventiva alla Banca d'Italia;
- le competenze per re-internalizzare le attività.

Per quanto concerne l'esternalizzazione delle funzioni aziendali di controllo, il Documento per la consultazione limitava alle sole banche, società di revisione o organismi associativi di categoria, il novero dei soggetti a cui affidare lo svolgimento di tali funzioni (cfr. Documento per la consultazione, Capitolo 7, Sezione IV, par. 1).
I rispondenti alla consultazione hanno chiesto di eliminare la disposizione in parola e di definire i requisiti di professionalità, indipendenza e organizzazione di cui il fornitore di servizi deve essere provvisto per assumere l'incarico.
La Banca d'Italia ha mantenuto l'impostazione della norma e ha chiarito che tale previsione trova giustificazione nella delicatezza dello svolgimento delle attività di controllo. In tal senso l'affidamento di tali funzioni è consentito solo a soggetti che già istituzionalmente svolgono attività bancarie o attività di controllo sulle banche. Sono, inoltre consentite forme di esternalizzazione verso organismi associativi, riconoscendo il ruolo di supporto di tali organismi verso le banche di minore dimensione.

Il Documento per la consultazione introduceva, inoltre, l'obbligo di informativa preventiva alla Banca d'Italia dell'intenzione di esternalizzare lo svolgimento, anche parziale, di FOI o di funzioni di controllo (cfr. Documento per la consultazione, Capitolo 7, Sezione IV, par. 1).
È stato chiesto, a tale riguardo, di limitare tale obbligo alle sole esternalizzazioni presso soggetti con sede in paesi extra UE.

La Banca d'Italia ha valutato in senso negativo tale richiesta, sostenendo che l'esternalizzazione incide in maniera rilevante sull'assetto organizzativo delle banche e, pertanto, l'obbligo di comunicazione preventiva deve valere indipendentemente dal paese in cui è inserito il fornitore di servizi.

Il ricorso all'outsourcing di funzioni aziendali era ammesso a condizione che le banche che ricorrono all'esternalizzazione mantenessero, tra le altre cose, le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, lo svolgimento delle funzioni esternalizzate (cfr. Documento per la consultazione, Capitolo 7, Sezione IV, par. 1).
L'obbligo di mantenimento di cui sopra è stato criticato soprattutto da parte delle banche di ridotte dimensioni, le quali hanno lamentato che ne deriverebbero costi troppo elevati che inficerebbero la convenienza del ricorso all'esternalizzazione. È stato, quindi, proposto di limitare l'obbligo al mantenimento delle conoscenze per affidare il servizio ad altro fornitore di servizi. Inoltre, è stato chiesto di chiarire modalità e termini per l'eventuale re-internalizzazione delle attività.
La Banca d'Italia ha valutato in senso negativo le osservazioni avanzate e ha mantenuto, pertanto, l'obbligo di trattenere le competenze necessarie per poter re-internalizzare, in caso di necessità, le funzioni esternalizzate. L'Autorità ha puntualizzato che il mantenimento delle competenze suddette risulta essere necessario, non solo per consentire l'effettività dei controlli sul fornitore di servizi, ma anche per non arrecare pregiudizio all'operatività aziendale nei casi in cui sia necessaria una re-internalizzazione. La Banca d'Italia ha specificato che, in generale, la valutazione delle competenze ritenute effettivamente necessarie è, innanzitutto, rimessa all'intermediario stesso. A titolo esemplificativo, nel caso di esternalizzazione delle funzioni di controllo, le competenze da mantenere possono consistere nella conoscenza e capacità di utilizzo delle metriche usate per la valutazione dell'esposizione ai rischi o delle regole e procedure oggetto di verifica da parte della funzione di compliance.

3.2 Il regime transitorio e la gap analysis

Le Disposizioni sono entrate in vigore il 3 luglio 2013, giorno di pubblicazione sul sito internet della Banca d'Italia del loro testo integrale, e saranno efficaci, fatte salve talune eccezioni, a partire dal 1° luglio 2014. L'adeguamento alle novità introdotte con questo intervento normativo presuppone, infatti, interventi significativi sulla struttura organizzativa, che richiedono tempo per essere realizzati. Pertanto, l'efficacia della nuova disciplina slitta, con riferimento a particolari disposizioni, fino al 1° luglio 2016. L'Autorità di vigilanza ha, comunque, richiesto alle banche di effettuare un'autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa (c.d. gap analysis) e di individuare le misure da adottare per assicurarne il rispetto[109].

Il presente paragrafo analizza le date entro le quali le banche sono chiamate a conformarsi alle disposizioni contenute nei Capitoli 7, 8 e 9 del Titolo V della Circolare 263/2006 (par. 3.2.1), e riporta le riflessioni sul Capitolo 7 condotte dall'ABI nell'ambito dello svolgimento di un'iniziativa di confronto tra le banche (par. 3.2.2).

3.2.1 Le date di efficacia delle nuove disposizioni

Le banche sono tenute a conformarsi alle disposizioni contenute nel Capitolo 7 entro il 1° luglio 2014, fatto salvo quanto segue:

- con riferimento alle funzioni aziendali di controllo di 2° livello (risk management e compliance), quanto previsto dalla Sezione III, par. 1, lett. b), secondo alinea, secondo periodo (linee di riporto dei responsabili di tali funzioni) sarà efficace a partire dal 1° luglio 2015;

[109] Cfr. Banca d'Italia, *Sintesi per gli utenti*, op. cit.

- con riferimento all'esternalizzazione di funzioni aziendali, disciplinata dalle Sezioni IV e V, le banche sono tenute ad adeguare i contratti di esternalizzazione in essere alla data di entrata in vigore delle Disposizioni alla prima scadenza contrattuale e comunque entro tre anni dall'entrata in vigore, ossia entro il 1° luglio 2016[110].

Le disposizioni contenute nei Capitoli 8 e 9 saranno efficaci, relativamente, a partire dal 1° febbraio 2015 e dal 1° luglio 2014. Tuttavia, per quanto riguarda l'adeguamento dei contratti di esternalizzazione del sistema informativo (Capitolo 8, Sezione VI) in essere alla data di entrata in vigore delle Disposizioni, la Banca d'Italia richiede alle banche di conformarsi, come previsto per le previsioni contenute nelle Sezioni IV e V del Capitolo 7, alla prima scadenza contrattuale e comunque entro tre anni dall'entrata in vigore (1° luglio 2016)[111].

3.2.2 Il documento di autovalutazione (gap analysis)

Come sopra meglio indicato, la data di efficacia delle nuove disposizioni in materia di sistema di controlli interni è fissata, salve le eccezioni di cui si è detto, al 1° luglio 2014.
Cionondimeno, i destinatari della disciplina, sin dall'entrata in vigore delle Disposizioni, hanno dovuto pianificare gli interventi da porre in essere ai fini dell'adeguamento al nuovo testo normativo.
La pianificazione condotta è stata necessaria anche a motivo delle richieste avanzate dalla Banca d'Italia, la quale ha, infatti, imposto alle banche l'invio di una relazione recante un'autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa (c.d. gap analysis), nonché le misure da adottare e la relativa scansione temporale per assicurare il pieno rispetto delle Disposizioni. Di seguito, per semplicità, indicheremo tale relazione anche con la dicitura Documento di gap analysis. La Banca d'Italia ha, inoltre, richiesto alle banche di comunicare i contratti di esternalizzazione in essere alla data di entrata in vigore delle Disposizioni e la relativa durata[112].

Originariamente, il Documento di gap analysis e la comunicazione dei contratti di esternalizzazione dovevano essere inviati alla Banca d'Italia entro il 31 dicembre 2013[113].
Con la Nota del 6 dicembre 2013 la Banca d'Italia ha, però, riposizionato la scadenza prevista per l'invio sia degli esiti della gap analysis sui Capitoli 7, 8 e 9, sia della comunicazione dei contratti di esternalizzazione, prorogando il termine dello stesso al 31 gennaio 2014.
Nella citata nota la Banca d'Italia ha comunicato di avere predisposto e reso disponibile un questionario per agevolare le banche nella comunicazione dei risultati della gap analysis sulle previsioni normative di cui ai Capitoli 8 e 9.

A supporto dell'effettuazione della gap analysis in materia di sistema dei controlli interni è, invece, intervenuta l'ABI, la quale ha avviato un'attività per certi versi propedeutica allo svolgimento da parte delle banche dell'autovalutazione della propria situazione rispetto alla disciplina contenuta nel Capitolo 7. Anche in base a contatti informali avuti con singole banche, l'ABI ha, infatti, ritenuto opportuno avviare un'iniziativa diretta ad individuare ed approfondire alcune tematiche particolarmente innovative nello specifico quadro del sistema dei controlli interni, rispetto alle quali si sentiva l'esigenza di confronto tra le banche[114].

[110] Cfr. Banca d'Italia, *Bollettino di vigilanza n. 7*, luglio 2013.
[111] *Ibid*.
[112] *Ibid*.
[113] *Ibid.*
[114] Analoga iniziativa è stata attivata sui Capitoli 8 e 9 da ABILab, il Centro di Ricerca e Innovazione per la Banca promosso dall'ABI.

Questa attività è stata svolta con la collaborazione di un apposito gruppo di lavoro interbancario, che nel corso di un primo incontro ha individuato i seguenti 4 ambiti meritevoli di approfondimento:

1. il coordinamento tra funzioni e organi con compiti di controllo;
2. i criteri per la definizione delle OMR;
3. l'esternalizzazione delle funzioni aziendali;
4. la verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni creditizie.

I primi tre temi sono stati affrontati in appositi sottogruppi, mentre il quarto ha visto la compartecipazione dei sottogruppi 1 e 2.
Il lavoro dei sottogruppi si è svolto in una serie programmata di incontri, che hanno permesso di consegnare l'output dell'analisi all'intero settore bancario in tempo utile per meglio individuare, nei propri Documenti di gap analysis, le linee di intervento da comunicare alla Banca d'Italia entro l'originaria scadenza del 31 dicembre 2013.
Il documento recante gli approfondimenti e le riflessioni in merito alle sopradette tematiche[115], di seguito, per semplicità, Documento ABI, è, infatti, stato inviato lo scorso 30 ottobre agli associati attraverso apposita lettera circolare.

Nel prosieguo del presente paragrafo verranno segnalate le osservazioni e le indicazioni avanzate dai sottogruppi in relazione alla disciplina nel suo complesso e alle prime tre tematiche oggetto di approfondimento[116], riportate all'interno del Documento ABI.

Per quanto concerne le osservazioni di carattere trasversale l'ABI si è preoccupata di ricordare che:

a) le Disposizioni si applicano alle banche sia a livello individuale che a livello consolidato e, pertanto, il Documento di gap analysis, pur dovendo essere redatto dalla capogruppo, doveva descrivere in modo esaustivo tutti i gap individuati a livello consolidato e a livello di banche controllate, le quali dovevano comunque procedere ad una sua formale approvazione;
b) le Disposizioni non si applicano alle componenti non bancarie del gruppo e quindi nella gap analysis le stesse devevano essere richiamate solo indirettamente ossia con riferimento ad eventuali gap riscontrabili nella complessiva struttura dei controlli di gruppo;
c) il livello di dettaglio della "scansione temporale" delle misure da adottare per colmare i gap non doveva essere eccessivamente granulare e comunque doveva essere commisurato al grado di definizione delle scelte effettuate dalla banca/gruppo in merito alle diverse opzioni di chiusura dei gap individuati; in altre parole, il grado di dettaglio doveva essere minore per soluzioni che al momento della redazione del Documento di gap analysis erano ancora in fase di progettazione.

Anche la Banca d'Italia ha fornito alcuni chiarimenti in materia di gap analysis nell'ambito della Nota del 24/01/2014 aggiornata in data 06/06/2014.
Oltre a confermare quanto già osservato dall'ABI e riportato al punto a) di cui sopra, la Banca d'Italia ha aggiunto, in merito, che ciascuna componente bancaria italiana del gruppo doveva redigere il proprio Documento di gap analysis ed era compito della capogruppo consolidare in un unico documento le analisi individuali e curarne la trasmissione all'Autorità di vigilanza.

[115] ABI, *Disposizioni Banca d'Italia. Nuovo sistema dei controlli interni. Riflessioni sul capitolo VII per la Gap Analysis*, Roma, 30 ottobre 2013.
[116] Si ritiene opportuno in questa sede non riportare le riflessioni condotte dai sottogruppi 1 e 2 in merito al compito della funzione di risk management di verificare il corretto svolgimento del monitoraggio andamentale sulle singole esposizioni creditizie. Per un apprendimento in materia si rinvia al Documento ABI.

In relazione al perimetro del documento consolidato di gap analysis, questione affrontata dall'ABI nei termini riportati al punto b) di cui sopra, la Banca d'Italia ha ritenuto opportuno fornire i seguenti chiarimenti:

- le componenti non bancarie e le controllate estere, non rientrando tra i destinatari delle Disposizioni ed essendo il Documento di gap analysis diretto a valutare il grado di aderenza alle stesse e a indicare le azioni per assicurarne il pieno rispetto, non erano tenute a redigere il documento di autovalutazione;
- la capogruppo, secondo quanto previsto dalla Sezione V del Capitolo 7, nel valutare l'adeguatezza del sistema dei controlli interni del gruppo, doveva tenere conto di tutte le componenti, incluse quelle non bancarie e le controllate estere, e doveva, altresì, esercitare i propri poteri di direzione e controllo per assicurare l'adeguatezza del sistema dei controlli di tali soggetti; ciò posto, il documento consolidato di gap analysis doveva dare conto della situazione dell'intero gruppo, incluse le componenti che non rientrano tra i destinatari della disciplina.

Ulteriori aspetti in materia di gap analysis di gruppo e di comunicazione dei contratti di esternalizzazione sono stati chiariti dalla Banca d'Italia nella sopracitata nota. L'Autorità di vigilanza ha, infatti, fatto presente che:

- le filiali di banche comunitarie erano tenute a effettuare la gap analysis con riferimento alle previsioni di cui sono destinatarie, che prevedono l'obbligo di condurre una verifica annuale circa l'adeguatezza delle procedure interne rispetto all'obiettivo di prevenire la violazione delle norme italiane applicabili alla succursale e la conformità della condotta aziendale rispetto alle stesse[117];
- l'elenco degli accordi di esternalizzazione in essere soggetti alle nuove Disposizioni doveva essere inviato dalla capogruppo;
- i contratti di esternalizzazione conclusi dopo l'entrata in vigore delle Disposizioni ma prima della loro data di efficacia dovevano essere adeguati alla nuova disciplina entro e non oltre quest'ultima data; entro la stessa data le banche dovevano inviare alla Banca d'Italia una comunicazione che indicasse tutti i contratti stipulati nel periodo compreso tra la data di entrata in vigore delle Disposizioni e la data della loro efficacia.

Affrontando specificamente il lavoro di approfondimento avente ad oggetto il documento di coordinamento di organi e funzioni con compiti di controllo, di seguito, per semplicità, Documento, il sottogruppo 1 ha ritenuto opportuno premettere che le Disposizioni assegnano allo stesso un'importanza strategica, attribuendogli il fine di evitare sovrapposizioni e lacune e lo scopo ultimo di assicurare il corretto funzionamento del sistema dei controlli interni.
Il Documento, la cui approvazione doveva avvenire entro il 30 giugno 2014, deve precisare, come noto:

a) i compiti e le responsabilità delle funzioni e degli organi con compiti di controllo;
b) i flussi informativi tra le diverse funzioni/organi e tra queste e gli organi aziendali;
c) le modalità di coordinamento e di collaborazione tra funzioni e organi di controllo.

In merito, il Documento ABI riporta quanto individuato dal sottogruppo con riferimento ai contenuti e alla redazione del Documento.

Per quanto riguarda i contenuti, viene segnalato che le banche avrebbero dovuto prestare attenzione alla redazione di un Documento che disciplinasse, con un adeguato livello di dettaglio, gli aspetti di cui sopra, ed in particolare quanto ai punti b) e c). Richieste generiche di coordinamento e invito alla collaborazione e allo scambio non sempre potrebbero, infatti, essere sufficienti. Era, quindi, necessario stabilire momenti e modalità di incontro e

[117] Cfr. Banca d'Italia, *Circ. n. 263 del 27/12/2006,* op. cit., Titolo V, Capitolo 7, Sezione VII.

collaborazione, nonché dettagliare i contenuti minimi dei flussi informativi che i diversi soggetti si devono scambiare.

Il sottogruppo rileva che dalle ricognizioni effettuate è emersa l'importanza che il regolatore ha inteso conferire ai flussi informativi tra le funzioni aziendali di controllo e le altre funzioni che effettuano attività di controllo su ambiti specifici (ad es. il responsabile della sicurezza e del trattamento dei dati), e tra tutte queste e gli organi aziendali. L'azione del regolatore è stata dunque orientata a costruire un ambiente organizzativo caratterizzato da flussi informativi ad elevata fruibilità, in modo tale da disegnare un circuito informativo ad ampio spettro che può coinvolgere diversi segmenti, la cui ampiezza e densità dovevano essere declinati all'interno del Documento che l'organo con funzione di supervisione strategica è tenuto ad approvare.

Il sottogruppo segnala, altresì, che nell'ambito delle riflessioni effettuate si sono distinte due tipologie di flussi informativi: i c.d. flussi orizzontali e verticali. I primi sono riferiti alle collaborazioni e ai flussi informativi tra le funzioni aziendali di controllo, le funzioni di controllo[118] e le altre funzioni/unità organizzative con compiti di controllo o che possono contribuire al sistema dei controlli interni per quanto concerne la mitigazione di alcuni rischi[119]. La seconda tipologia di flussi è riferibile ai flussi informativi tra le tre categorie di funzioni sopra individuate e gli organi aziendali di controllo, il cui scopo è quello di fungere da supporto alle decisioni di questi ultimi.

Con riferimento alle collaborazioni e ai flussi informativi orizzontali, viene messa in evidenza la necessità che nel Documento, oltre a quanto indicato dalle Disposizioni e ricordato ai punti a), b) e c) di cui sopra, venissero:

- istituzionalizzati dei momenti di coordinamento in fase di programmazione periodica delle rispettive attività, allo scopo di presidiare correttamente tutti i potenziali rischi e individuare e gestire in maniera efficace le aree di sovrapposizione;
- disciplinati l'insieme dei flussi a scadenza prefissata o da attivare in presenza di specifiche evidenze emerse o di eventi particolari; questi flussi informativi orizzontali devono essere improntati a criteri di selettività, sinteticità e standardizzazione;
- stabiliti i casi in cui debba essere attivato un processo di analisi congiunta dei report aventi l'obiettivo di proporre a chi di competenza le diverse azioni di rimedio alle debolezze del sistema dei controlli interni individuate dai soggetti coinvolti;
- identificati soggetti, compiti e ruoli in relazione a macro-tipologie di particolari eventi quali visite ispettive, crisi reputazionali, ecc.;
- individuate eventuali attività di allineamento dei diversi soggetti rispetto alle tassonomie, dati e metriche.

Per quanto riguarda, invece, le collaborazioni e i flussi informativi verticali e in particolare le informazioni ricevute dalle funzioni aziendali di controllo, il sottogruppo precisa che, non essendo contemplata dalle Disposizioni una figura di coordinamento e di riporto delle funzioni di controllo di secondo livello[120], l'attività di coordinamento e integrazione dei flussi informativi, per la costruzione di una visione olistica ed integrata dei rischi e la realizzazione di una sintesi informativa da trasmettere al massimo organo societario, doveva essere affidata all'organo con funzione di supervisione strategica o all'organo con funzione di rispetto ai quali le due funzioni si trovano alle dirette dipendenze.

---

[118] Per le definizioni di "funzioni di controllo" si veda Banca d'Italia, *Circ. n. 263 del 27/12/2006*, op. cit., Titolo V, Capitolo 7, Sezione I, par. 3.

[119] Si tratta di funzioni/unità organizzative la cui mission prevalente non attiene all'esecuzione dei controlli; ad esempio legale, pianificazione, fiscale, risorse umane, privacy, sicurezza, ecc.

[120] La possibilità di istituire una figura di coordinamento dei controlli di secondo livello, cui riportino gerarchicamente i responsabili delle funzioni addette a tali controlli, è stata espressamente negata all'interno del Resoconto della consultazione della Banca d'Italia; vedi infra par. 3.1.2.

Sul fronte del coordinamento di tipo verticale, viene segnalato che una particolare attenzione andava prestata al rapporto tra l'O.d.V. e l'organo con funzione di controllo, e che a livello di Documento di gap analysis era necessario prevedere, qualora l'organo di controllo svolgesse le funzioni dell'O.d.V., le modalità chiare di esplicitazione dei loro interventi.

In merito alla redazione del Documento, il sottogruppo ricorda che la sua assenza doveva essere segnalata nel Documento di gap analysis, così come la previsione di aggiornamento di un Documento esistente ma non pienamente conforme nei contenuti alle Disposizioni, evidenziando i tempi previsti di realizzo.
Riguardo a quale funzione potesse collaborare alla redazione del Documento con l'organo preposto all'approvazione dello stesso, il sottogruppo rileva che dalle ricognizioni effettuate sono emerse anche soluzioni diverse da quella indicate nel Resoconto della consultazione della Banca d'Italia[121], che identificavano nell'organo con funzione di controllo l'organo cui sarebbe possibile attribuire il compito di coordinare le azioni e le analisi propedeutiche alla redazione del Documento. Era, inoltre, analogamente possibile affidare tale compito ai Comitati Inter-funzionali, piuttosto che all'Amministratore Incaricato.
Ciò posto, viene sottolineata la necessità, ferma restando l'ampia autonomia di ciascuna banca sulla soluzione da adottare, di prevedere una formalizzazione della funzione o dell'organo chiamato ad espletare l'attività di preparazione del Documento.

Passando a rendicontare quanto emerso dal lavoro di approfondimento svolto dal secondo sottogruppo, avente ad oggetto i criteri per l'individuazione delle OMR da sottoporre al vaglio preventivo della funzione di controllo dei rischi, il Documento ABI ricorda, primariamente, quanto già chiarito all'interno del Resoconto della consultazione da parte della Banca d'Italia. Come appare dalla lettura di quest'ultimo, non sarebbero OMR quelle operazioni che rientrano nelle competenze degli organi aziendali[122]. Il sottogruppo 2 sostiene, a tale proposito, che il risk management potrebbe essere chiamato dagli organi aziendali a fini consultivi per le OMR che gli stessi hanno evocato a sé. Ciò detto, il sottogruppo sottolinea che il senso della definizione delle OMR è però quello di permettere di intercettare e far confluire alla funzione di controllo dei rischi tutte quelle operazioni che potrebbero altrimenti non essere mai vagliate in ottica di risk management o esserlo solo in fase decisionale avanzata (ossia se e quando vagliate dagli organi e se questi consultano il risk management) se non addirittura a posteriori. Il sottogruppo afferma, infatti, che l'ottica del risk management sulle OMR deve essere ex-ante, ma soprattutto il risk management deve esprimersi preventivamente sulla coerenza delle stesse con il RAF.

I risultati del lavoro di approfondimento svolto hanno, inoltre, permesso di fornire indicazioni sui criteri quali-quantitativi da seguire per l'individuazione delle OMR.
Tali criteri, sostiene il sottogruppo, devono essere definiti e approvati dall'organo con funzione di supervisione strategica e le scelte da quest'ultimo effettuate impattano sia sul potere del risk management sia sulla sostenibilità dello stesso rispetto ad un numero eccessivamente elevato di richieste di parere preventivo.
Viene segnalata la necessità che i criteri di definizione delle OMR siano espressi in un linguaggio comprensibile ai più e che siano resi noti a tutte le componenti dell'organizzazione anche al fine di permettere alle funzioni proponenti OMR di effettuare in autonomia una sorta di pree-screening.
Sul fronte dei criteri quantitativi, il sottogruppo individua l'adozione di soglie prefissate per macro categorie di operazioni, il cui superamento determina l'individuazione delle OMR. Le soglie possono essere individuate in base ad una prima valutazione di massima dei principali profili di rischio oppure ad una più precisa analisi di sensitivity, effettuata su alcuni o su tutti i

[121] Vedi infra par. 3.1.2.
[122] Vedi infra par. 3.1.1

profili di rischio, avente comunque l'obiettivo di individuare l'ammontare dell'operazione tale per cui si possa parlare di OMR. Inoltre, viene segnalato il problema dell'aggiornamento delle soglie al variare delle situazioni di contesto e dell'opportunità di definire soglie dinamiche. Viene, infatti, sottolineata la necessità di rivalutare le soglie prefissate in relazione o al cumularsi di molteplici operazioni non OMR o in presenza di OMR che modificano il profilo di rischio (ad es. un'operazione di un determinato ammontare, sotto soglia in un determinato momento, potrebbe essere classificata come OMR se le soglie tenessero conto delle operazioni nel frattempo poste in essere).

Se i criteri quantitativi vengono superati ed una operazione diventa OMR, il sottogruppo ricorda che vanno comunque verificati gli aspetti di rischiosità espressi dai criteri qualitativi. Viceversa, anche quando i criteri quantitativi non sono violati, un'operazione può rientrare tra le OMR se soddisfa anche i soli criteri qualitativi. Vengono individuati, a titolo esemplificativo, i seguenti criteri qualitativi:

- operazioni con profili di rischio reputazionale;
- operazioni non tradizionali per la banca e innovative per le unità di business che le devono implementare;
- operazioni complesse con profilo di rischio non lineare;
- operazioni con legami diretti o indiretti con le remunerazioni del management;
- operazioni relative a partecipazioni in società non finanziarie o acquisizioni che non rientrano nella sfera dell'organo con funzione di supervisione strategica, ma potrebbero avere riflessi di rischio reputazionale.

In termini di gap analysis, il sottogruppo evidenza che la mancanza di una policy per le OMR era uno dei punti principali da affrontare e che, al suo interno, i criteri quantitativi devevano essere tradotti in una tassonomia chiara o, più in generale, dovevano essere introdotte delle specificazioni tendenti a ridurre il più possibile l'inevitabile aspetto soggettivo della valutazione dei profili qualitativi. Un primo tentativo in tal senso poteva essere quello di fornire una esemplificazione ispirata a casi teorici o a situazioni aziendali pregresse che sarebbero rientrate, al momento della definizione della politica aziendale, nelle OMR.

Il sottogruppo 3 ha affrontato il tema dell'esternalizzazione delle funzioni aziendali, e in particolare, ha analizzato, tra le altre, le seguenti tematiche:

- cosa non si intende per esternalizzazione;
- quali sono i criteri per la redazione della politica in materia di esternalizzazione;
- come individuare le diverse categorie di esternalizzazione;
- quale categoria di esternalizzazione comunicare alla Banca d'Italia;
- la re-internalizzazione.

Per quanto concerne la prima tematica, il sottogruppo considera non esternalizzate quelle attività che vengono affidate ad altri (infragruppo o terzi) in quanto non possono essere svolte nell'ambito della banca (es. produzione di energia elettrica, forniture di servizi che la banca non offre, contratti di consulenza, prestazioni professionali, offerta fuori sede quando non ci sono dipendenti iscritti all'Albo dei promotori finanziari, ecc.). Viceversa la banca esternalizza solo quando affida ad altri un'attività o una fase di attività che potrebbe svolgere al proprio interno.

In relazione ai criteri per la redazione della policy di esternalizzazione, che doveva essere approvata entro il 2 luglio 2014, oltre a riportare quanto stabilito dalle Disposizioni in merito proprio ai contenuti della stessa, sono state fornite le seguenti indicazioni:

- la politica deve contenere le linee guida per tutte le tipologie di esternalizzazione di funzioni aziendali (anche non importanti e non di controllo), sia infragruppo sia verso terzi;

- è possibile inserire un cappello iniziale che regolamenti i principi generali della pratica dell'esternalizzazione (ad es. etici) nonché di richiamo delle politiche pertinenti come ad esempio quella in tema di conflitti di interesse;
- la politica deve definire la modalità per la determinazione del tipo di esternalizzazione e del livello di importanza; in alcune realtà è già attivo un tavolo inter funzionale di valutazione delle esternalizzazioni (controllo rischi, compliance, organizzazione e centri di responsabilità) che ne analizza sostanzialmente la maggior parte;
- la politica deve individuare i criteri per l'individuazione della tipologia di contratti che possono o meno prevedere gli accordi di sub esternalizzazione e, se del caso, le caratteristiche della sub esternalizzazione medesima;
- la politica deve disciplinare i criteri e il processo interno per la definizione delle funzioni operative importanti.

Per quanto concerne la gap analysis, il sottogruppo evidenzia che la stessa doveva compiersi comparando l'attuale policy aziendale con quella delineata dalle nuove Disposizioni

Al fine di individuare le diverse categorie di esternalizzazione, il sottogruppo è partito dalle definizioni di "esternalizzazione", "funzione aziendale" e "funzione operativa importate" fornite dalle Disposizioni, per individuare il sottoinsieme delle esternalizzazioni di funzioni aziendali e tra queste, attraverso un'opera di ulteriore filtraggio, le esternalizzazioni di FOI.
Il sottogruppo identifica, quindi, le esternalizzazioni di funzioni aziendali in quelle strettamente connesse all'attività tipica della banca, che comportano, pertanto, un possibile rischio (operativo, di non conformità, reputazionale e strategico) (ad es. servizi di fatturazione o di formazione del personale), e tra queste definisce esternalizzazioni di FOI solo quelle relative a funzioni aziendali che comportano un livello di rischio maggiore (ad es. back office, servizio archivio, recupero crediti, sistema informativo, trattamento del contante, gestione patrimoni, funzioni di controllo, ecc.). Il sottogruppo precisa, però, che ogni banca, in funzione della propria realtà aziendale e del proprio modello organizzativo di business, deve individuare le proprie esternalizzazioni di FOI, tenendo conto anche di criteri quantitativi quali ad esempio il valore dell'attività esternalizzata.

Secondo il parere del sottogruppo sono oggetto di analisi da parte del Regulator la policy in materia di esternalizzazione e la valutazione complessiva dell'aderenza alla stessa, mentre il processo di verifica del singolo contratto di esternalizzazione viene effettuato solo per le FOI. Pertanto, la comunicazione da inoltrare alla Banca d'Italia entro l'originaria scadenza del 31 dicembre 2013, in base alla suddetta interpretazione, doveva limitarsi ai soli contratti di esternalizzazione di FOI, costituendo così l'archivio presso la Banca d'Italia delle esternalizzazioni di questa categoria di funzioni che nel tempo sarebbe stato aggiornato con le comunicazioni preventive.
Tuttavia, appare opportuno rilevare che l'Autorità di vigilanza, sia nel disporre l'obbligo di comunicare i contratti di esternalizzazione in essere alla data di entrata in vigore delle Disposizioni, sia nella Nota di chiarimenti del 24/01/2014 aggiornata in data 06/06/2014, non si esprime circa la categoria di esternalizzazione oggetto della comunicazione. Rimarrebbe, quindi, da verificare se le banche hanno sposato l'interpretazione dell'ABI o hanno preferito comunicare i contratti di esternalizzazione in essere senza fare distinzione di categoria.

Infine, il Documento ABI riporta anche le osservazioni avanzate dal sottogruppo 3 in relazione alla necessità per le banche di mantenere le competenza tecniche e gestionali per re-internalizzare.
Nel caso di esternalizzazione infragruppo, il sottogruppo sostiene che le capacità rimanenti in capo a chi ha esternalizzato, nei confronti del quale le Disposizioni non prevedono il rispetto dell'obbligo di cui sopra, dovrebbero limitarsi alla possibilità di svolgere adeguatamente una valutazione circa l'opportunità di re-internalizzare o affidare a terzi il servizio non più svolto dalla capogruppo o dalla società del gruppo.

In caso, invece, di esternalizzazione verso terzi, il sottogruppo afferma che la policy dovrebbe identificare i casi in cui il rischio di re-internalizzazione è particolarmente alto (ad es. per caratteristiche imputabili al fornitore), mentre negli altri casi sarebbe opportuno mantenere le competenze per il controllo e dotarsi di procedure formalizzate necessarie a gestire i casi di affidamento ad altri fornitori dei servizi per i quali risulta improponibile la re-internalizzazione.

CAPITOLO 4

Unicredit, UBI Banca e Banca Popolare di Sondrio: sistemi di controllo interno a confronto

4.1 La classifica sulla governance del RiskGovernance Group

I temi della corporate governance e del risk management sono prepotentemente divenuti i protagonisti delle cronache mondiali nel periodo della crisi, suscitando un forte interesse anche tra un pubblico non specializzato. Le carenze mostrate hanno rivelato l'importanza di valutare i sistemi di governo societario e di gestione dei rischi delle banche.

Si è occupato del tema il centro di ricerca in ambito *Risk Management & Corporate Governance* del Politecnico di Milano, che ha concluso negli ultimi mese del 2013 un ampio studio sulla Corporate Governance nel settore bancario di quattro paesi europei.
Lo studio ha elaborato i dati rilevati nel triennio 2010 – 2012 inerenti 32 istituti di credito quotati in Italia, Spagna, Francia e UK e ha utilizzato quale strumento di valutazione il *CGBI - Corporate Governance Banking Index*, appositamente ideato per il settore bancario dallo stesso *RiskGovernance Group*.
L'indice prende origine dal *CGI - Corporate Governnace Index* realizzato nel 2008 e utilizzato in questi anni per misurare la qualità del sistema di governo societario delle imprese quotate in Italia e all'estero.
Lo studio ha analizzato la relazione tra *CGBI* e valore, evidenziando che alle banche con migliore governance è associato anche un valore maggiore, ovvero che investire in Corporate Governance premia.
Inoltre il *RiskGovernnace Group* ha elaborato, sulla base dei risultati dell'analisi svolta, la classifica delle 30 banche con la governance migliore. Occupa la prima posizione Société Générale, seguita da Barclays e Royal Bank of Scotland. Delle italiane, la prima è Unicredit al settimo posto, seguita da Intesa San Paolo al decimo e da Monte dei Paschi di Siena all'undicesimo. La classifica complessiva è riportata nella Figura 1.

Figura 1: *La classifica della Governance*

Banca	CGBI©	Banca	CGBI©
Société Générale	81,19	Credito Valtellinese	61,76
Barclays	78,82	UBI	60,24
Royal Bank of Scotland	76,47	Banca Profilo	59,80
BNP Paribas	76,12	Banco Desio Brianza	59,19
Crédit Agricole	73,96	Natixis	58,44
Standard Chartered	73,76	Banca Finnat	57,26
Unicredit	73,38	Banco Popular Español	56,72
HSBC	71,53	Banca Carige	56,43
Lloyd's	68,82	Banca Popolare Milano	55,29
Intesa Sanpaolo	65,24	BBVA	55,07
Banca MPS	64,35	Banca Popolare Emilia Romagna	54,71
Banco Popolare	63,38	Banca Popolare Etruria-Lazio	53,29
Santander	62,92	Bankinter	52,36
Mediobanca	62,79	Banco de Sabadell	49,21
Credito Emiliano	62,35	Banca Popolare di Sondrio	34,31

Fonte: Ferrando M., *Banche, italiane fuori dal podio nella classifica della governance*, Il Sole 24 ORE, 11 dicembre 2013.

Su un totale di 16 istituti domestici, solo 6 occupano posizioni nella prima colonna della classifica, mentre più della metà figurano nella seconda parte. Tuttavia, piazzare 16 banche su 30 all'interno della classifica delle banche con la migliora governance fa emergere senza dubbio gli sforzi condotti dagli istituti italiani.

Il presente capitolo cerca di fornire un quadro sintetico della struttura dei controlli interni di Unicredit, la banca italiana più "virtuosa" sul tema della governace, di UBI Banca, che ha occupato esattamente la posizione intermedia tra le 16 banche del nostro paese, e di Banca Popolare di Sondrio, ultima tra le domestiche e tra le 30 classificate.

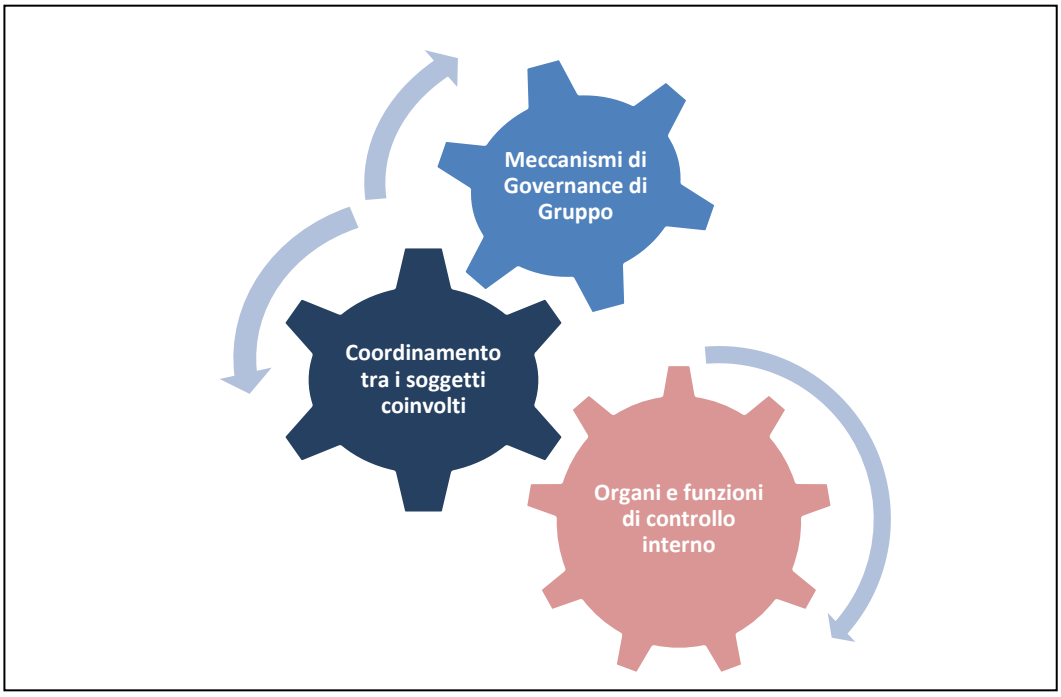
Le informazioni esposte sono rilevabili per lo più dalla *Relazione sul governo societario e sugli assetti proprietari* redatta per l'anno 2013 da ciascuna delle tre banche scelte per il confronto.
Pertanto, le informazioni riportate dipendono da ciò che stesse hanno comunicato ai propri stakeholders: potrebbero, quindi, essere state fornite, con riferimento a particolari aspetti del sistema dei controlli interni, spiegazioni dettagliate delle proprie regole di governance del rischio che nella realtà magari non trovano completa applicazione; così come l'assenza di informazioni potrebbe dipendere dalla mancata disclosure sull'architettura dei controlli interni.

4.2 Unicredit

> *"Un sistema dei controlli interni efficace ed efficiente è, di fatto, il presupposto per la creazione di valore nel medio lungo termine, per la salvaguardia della qualità delle attività, per una corretta percezione dei rischi ed un'appropriata allocazione del capitale*".

Il quadro del sistema dei controlli interni del Gruppo si fonda sui tre elementi rappresentati in Figura 1.

Figura 1 : Unicredit – *Le componenti del sistema dei controlli interni*



Il sistema dei controlli interni del Gruppo coinvolge i seguenti organi/funzioni:
- il Consiglio di Amministrazione e il Comitato per i Controlli Interni & Rischi;
- l'Amministratore incaricato del sistema dei controlli interni e di gestione dei rischi;
- il Collegio Sindacale e l'O.d.V. ex d.lgs. 231/2001;
- le funzioni aziendali di controllo.

> *"Il miglioramento dell'interazione tra funzioni di controllo e il costante aggiornamento agli organi aziendali da parte delle stesse in relazione alle attività svolte hanno la finalità ultima di costituire nel tempo una governance aziendale che garantisca la sana e prudente gestione anche attraverso un più efficace presidio del rischio a tutti i livelli aziendali".*

Con l'obiettivo di evitare quanto più possibile sovrapposizioni e lacune sono state, pertanto, disegnate, all'interno del framework più generale di attiva e costante collaborazione, formalizzato in specifici regolamenti interni, le modalità di interazione e coordinamento tra funzioni e organi aziendali coinvolti nel sistema dei controlli di Unicredit.
Nello specifico, Unicredit ha rafforzato in maniera significativa le forme di collaborazione e coordinamento tra le funzioni di controllo, attraverso la formalizzazione nelle relative normative interne dei flussi informativi da implementare.

> *"Un efficace sistema dei controlli interni si basa su adeguati meccanismi di governance mediante i quali Unicredit, in qualità di Capogruppo, esercita la direzione ed il coordinamento delle Società del Gruppo [...]*".

Rilievo importante assumono, quindi, anche i meccanismi di governance di Gruppo di Unicredit, nell'ambito dei quali la Società agisce attraverso:

- l'individuazione di *fiduciari* negli organi sociali e nelle posizioni manageriali delle società appartenenti al Gruppo;
- un sistema manageriale/funzionale di Gruppo, creato dalle c.d. *GMGR – Group Managerial Golden Rules*, che definisce i meccanismi di coordinamento manageriale, attribuendo ai Rsponsabili delle funzioni di Unicredit specifiche responsabilità nei confronti delle corrispondenti funzioni delle società appartenenti al Gruppo;
- il monitoraggio dell'adozione da parte delle società delle regole di Gruppo, c.d. *Global Rules*, emanate da Unicredit per disciplinare, tra l'altro, attività rilevanti per la gestione dei rischi, nonché al fine di assicurare unitarietà di indirizzo al disegno imprenditoriale e all'operatività complessiva;
- la diffusione di best practices all'interno del Gruppo con lo scopo di uniformare le modalità operative per il migliore presidio dei rischi e per una maggiore efficienza operativa.

Le *GMGR* definite da Unicredit creano, come sopra anticipato, un sistema di gestione manageriale e funzionale che interessa l'intero Gruppo e che opera in maniera trasversale rispetto alle strutture societarie che lo compongono. All'interno di questo sistema operano, creando un forte legame funzionale tra le strutture di Capogruppo e le corrispondenti strutture delle società del Gruppo, le *Competence Line*, rappresentate dalle strutture/funzioni aventi l'obiettivo di indirizzare, coordinare e controllare le attività ed i rischi del Gruppo nel suo complesso e delle singole società[123].
I Responsabili delle Competence Line assicurano, altresì, il monitoraggio dell'adozione delle Global Rules da parte delle società del Gruppo.

Al fine di disporre di una visione organica dell'interno sistema dei controlli di Unicredit, si affrontano, nel prosieguo, i principali protagonisti del sistema dei controlli interni della Società elencati in precedenza, suddividendoli tra organi e funzioni aziendali di controllo.

[123] A titolo esemplificativo si citano Planning, Finance & Amministration, Risk Management, Legal & Compliance e Internal Audit.

4.2.1 Gli organi aziendali coinvolti nel sistema dei controlli interni

Di fondamentale importanza l'operato svolto dal Consiglio di Amministrazione[124] nell'ambito del sistema dei controlli interni del Gruppo all'interno del quale l'organo in questione definisce le linee di indirizzo del sistema stesso.
In tale contesto, nel corso del 2013, il Consiglio ha approvato il *RAF* di Gruppo per l'anno 2014 al fine di garantire che il business si sviluppi nell'ambito del corretto profilo di rischio[125].
Il Consiglio ha approvato, inoltre, la costituzione delle funzioni aziendali di controllo, delineandone ruoli e responsabilità, ed ha incaricato il *CEO - Chief Executive Officer*[126] di progettare, gestire e monitorare il sistema dei controlli interni.
Il Consiglio di Unicredit, avvalendosi dell'operato del *Comitato per i Controlli Interni & Rischi*, svolge, altresì, un'attività di supervisione complessiva dei principali rischi aziendali e di valutazione, almeno annualmente, dell'adeguatezza, della funzionalità e dell'efficacia del sistema dei controlli interni.
Con specifico riferimento al rischio di non conformità, il Consiglio, sentito il Collegio Sindacale, approva le politiche di gestione del rischio stesso, valuta, almeno una volta l'anno, avvalendosi del supporto tecnico del *Comitato per i Controlli Interni & Rischi*, l'adeguatezza della struttura organizzativa, la qualità e quantità delle risorse della funzione di compliance, nonché analizza le relazioni periodiche concernenti le verifiche dalla stessa effettuate nell'ambito della gestione del rischio di non conformità.

L'istituzione dell'attuale *CCI&R - Comitato per i Controlli Interni & Rischi*[127] di UniCredit risale al giugno 2000 quale Comitato Audit. Nel corso degli anni la denominazione originaria ed i relativi compiti sono variati, in linea con l'evoluzione del quadro regolamentare, nonché delle best practices. La composizione e le competenze del Comitato, come quelle degli altri comitati consiliari, sono stabilite nel Regolamento del C.d.a.
Il Comitato si riunisce sia in seduta plenaria che a composizione ristretta, nell'articolazione in due Sotto-Comitati focalizzati su tematiche diverse:
- *Sotto-Comitato per i Controlli Interni* che si occupa dei controlli interni del Gruppo;
- *Sotto-Comitato per i Rischi* che si occupa dei rischi del Gruppo.

Il Comitato si riunisce almeno una volta al mese, in base ad una precisa pianificazione annuale: almeno due volte l'anno in seduta plenaria, a mesi alterni in composizione ristretta. In ogni caso le riunioni sono indette quando necessario per discutere gli argomenti di competenza.
Alle riunioni partecipano, in qualità di invitati permanenti, il *CEO*, il Direttore Generale, i Responsabili della funzione di Internal Audit e Compliance, il *GCRO - Group Chief Risk Officer* e il *GCFO - Group Chief Financial Officer*.
Il Comitato riferisce al Consiglio sull'attività svolta dopo ogni riunione e almeno semestralmente sull'adeguatezza del sistema dei controlli interni.
Nel corso dell'esercizio 2013 si è riunito 14 volte, mentre per il 2014 sono state pianificate 12 riunioni.

[124] Unicredit adotta il sistema di amministrazione e controllo cosiddetto tradizionale basato sulla presenza di due organi di nomina assembleare: il Consiglio di Amministrazione, con funzioni di supervisione strategica e di gestione dell'impresa, ed il Collegio Sindacale, con funzioni di controllo sull'Amministrazione.
[125] Vedi infra par. 4.2.4.
[126] L'unico consigliere di Unicerdit che ha ricevuto deleghe gestionali è l'Amministratore Delegato della società, responsabile della gestione dell'impresa. Nel Consiglio non vi sono consiglieri, oltre al CEO, definibili come esecutivi. L'Amministratore Delegato ricopre, pertanto, l'importante ruolo assegnato dalla disciplina all'organo con funzione di gestione. Si veda infra par. 2.1.2.
[127] Il Comitato per i Controlli Interni & Rischi di Unicredit rappresenta una dei 5 comitati consiliari aventi finalità consultive e propositive in relazione a diversi ambiti di competenza, costituiti all'interno del Consiglio di Amministrazione.

Il *CCI&R* svolge i compiti allo stesso demandati dal C.d.a., operando con funzioni consultive e propositive a supporto di quest'ultimo relativamente alle materie concernenti il sistema dei controlli interni.
In particolare, assiste il Consiglio nella definizione delle linee di indirizzo del sistema dei controlli interni, nonché nella formalizzazione delle politiche per il governo dei rischi e nel loro riesame periodico, nella vigilanza sul concreto funzionamento dei processi di gestione e controllo dei rischi, nella determinazione dei criteri di compatibilità dei rischi aziendali con una sana e corretta gestione della società, nella verifica periodica dell'adeguatezza, dell'efficacia e dell'effettivo funzionamento del sistema medesimo, assicurando che i principali rischi aziendali siano correttamente identificati, misurati, gestiti e monitorati in modo adeguato.
Inoltre il Comitato, al fine di supportare il Consiglio di Amministrazione nei compiti allo stesso demandati:

- analizza le linee guida di Gruppo per le attività di Audit e valuta l'adeguatezza del piano annuale dei controlli predisposti dal Responsabile della funzione di Internal Audit;
- può richiedere l'effettuazione di specifici interventi di Audit;
- valuta il lavoro svolto dalla società di revisione del Gruppo;
- si esprime in merito alla nomina o alla sostituzione del Responsabile della funzione di Internal Audit e del Responsabile della funzione di Compliance;
- è incaricato di esaminare l'assessment in tema di rischi a livello di Gruppo;
- vigila affinché la funzione di Compliance applichi le politiche di gestione del rischio di non conformità definite dal Consiglio, monitorandone recepimento e implementazione;
- effettua l'analisi delle relazioni periodiche predisposte dalle funzioni aziendali di controllo, valutandone gli eventuali rilievi;
- analizza le relazioni sulle attività svolte dal *I.C.C.C. – Internal Controls Coordination Committee* (Comitato Manageriale di Coordinamento Controlli);
- è incaricato dell'esame dell'adeguatezza, sotto il profilo quali/quantitativo, delle strutture organizzative delle funzioni di Compliance e Internal Audit.

Nel 2013, sotto la forte sponsorship del Presidente del *CCI&R*, sono state portate avanti e consolidate due iniziative aventi lo scopo di coordinare il sistema dei controlli del Gruppo e contribuire fattivamente alla diffusione della cultura del rischio all'interno del Gruppo.
In particolare si è riunito due volte il *Group Audit Committee Chairmen Council*, con la finalità di condividere le tematiche rilevanti e trasversali in tema di sistema dei controlli e di gestione dei rischi. Il Council è composto dal Presidente del *CCI&R* di Unicredit e dai Presidenti degli omologhi Comitati istituiti presso le principali partecipate. Partecipano al Council anche il Presidente del C.d.a. e del Collegio Sindacale, nonché il Direttore Generale e il Responsabile della funzione di Internal Audit di Unicredit.
Si è inoltre tenuto l'annuale incontro del Comitato con i *Country Chairmen* e i *CEO* delle principali società del Gruppo.

L'Amministratore Delegato, nel prosieguo anche *CEO*, come incaricato dal C.d.a., gestisce il sistema dei controlli interni e di gestione dei rischi. In tale contesto:

- identifica i principali rischi aziendali, sottoponendoli all'esame del Consiglio;
- attua gli indirizzi del C.d.a. attraverso la progettazione, la gestione ed il monitoraggio del sistema dei controlli interni e di gestione dei rischi avvalendosi delle competenti funzioni; nello svolgimento di tali attività, il CEO è supportato dal Direttore generale, il quale preside l'*ICCC - Internal Control Coordination Committee* nel quale vengono affrontate le tematiche inerenti il sistema dei controlli interni nonché i piani di rimedio ad esse collegati.

Nell'ambito delle riunioni del *CCI&R*, il *CEO*, in qualità di invitato permanente, riferisce sulle tematiche poste all'ordine del giorno, fornendo i chiarimenti richiesti e accogliendo le eventuali richieste di approfondimento del Comitato stesso.

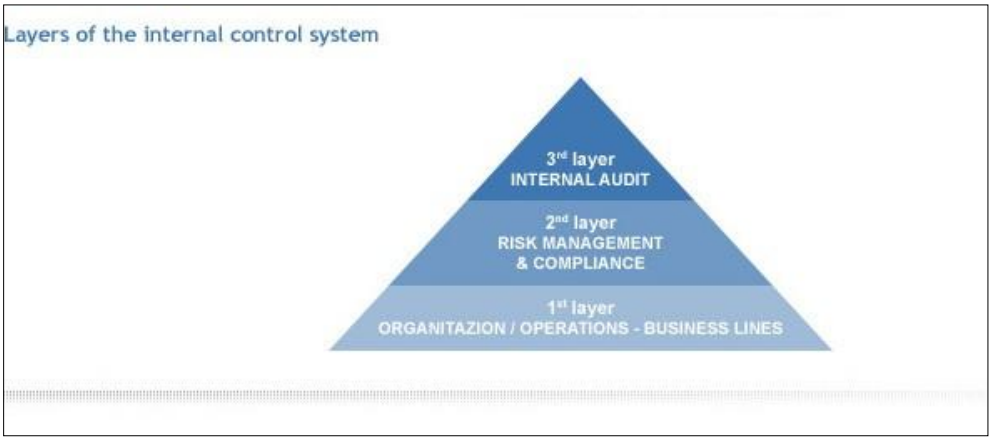
Particolari compiti sono assegnati all'Amministratore Delegato con specifico riferimento al rischio di conformità. Il *CEO* deve, infatti, assicurare l'efficace gestione del rischio in questione, predisponendo adeguate policy e procedure per la conformità alla normativa vigente, accertando, in caso di violazioni, che siano apportati i rimedi necessari e delineando flussi informativi volti a garantire ai competenti organi aziendali piena consapevolezza sulle modalità di gestione del rischio di non conformità. Con il supporto della funzione di Compliance, il *CEO* identifica e valuta almeno annualmente i principali rischi di non conformità a cui il Gruppo è esposto e programma i relativi interventi di gestione, nonché riferisce al Consiglio e al Collegio Sindacale almeno una volta l'anno sull'adeguatezza della gestione del rischio di non conformità.

Svolge compiti di vigilanza sull'efficacia del sistema dei controlli interni e di gestione dei rischi il Collegio Sindacale[128] di Unicredit. Per quanto concerne l'attribuzione al Collegio anche delle funzioni di O.d.V. ex d.lgs. 231/2001, come previsto dal 15° aggiornamento del 2 luglio 2013 alla Circolare 263/2006, Unicredit ha mantenuto l'assetto previgente continuando ad esistere un Organismo appositamente costituito per lo svolgimento di tali funzioni.

4.2.2 Le funzioni aziendali di controllo

Unicredit monitora, misura e controlla l'insieme dei rischi del Gruppo attraverso i tre livelli tipici del controllo, come mostra la Figura 2.

Figura 2 : Unicredit – *I livelli del sistema dei controlli interni*



Fonte: sito web www.unicreditgroup.eu

Nell'ambito dei controlli di 1° livello, effettuati dalle stesse strutture operative o incorporati dalle procedure o eseguiti dal back office, Unicredit ha istituito una struttura dedicata denominata *Internal Controls Italy* che supporta il *Country Chairman Italy* in qualità di responsabile del sistema dei controlli operativi di primo livello.

I controlli di 2° livello sono, invece, affidati a unità diverse da quelle produttive. Le Direzioni responsabili dei controlli di 2° livello sono la funzione di *Compliance*, all'interno del *Legal & Compliance Department*, e il *Group Risk Managament*.

Nell'ambito del quadro che va definendosi il tema della governance del rischio merita un focus a parte. Tralasciamo, infatti, in questa sede l'inquadramento della funzione di Risk Management del Gruppo di cui ci occuperemo nel paragrafo successivo.

Come sopra detto, i controlli sulla conformità sono affidati alla funzione di Compliance che ha un'organizzazione sia globale, per mezzo della Direzione denominata *Department Global Compliance* di Unicredit, sia locale all'interno delle singole società del Gruppo.

[128] Il Collegio Sindacale di Unicredit ricopre l'importante ruolo assegnato dalla disciplina all'organo con funzione di controllo. Si veda infra par. 2.1.2.

Presiede il *Department* il *GCO - Group Compliance Officer*, nominato dal C.d.a. di Unicredit, previo parere del Collegio Sindacale.
L'estensione del presidio di Complance in ciascuna società del Gruppo è determinata da fattori quali la tipologia e la complessità dell'attività svolta o dei servizi offerti e la dimensione della società stessa. È, infatti, prevista la possibilità di avere una presenza della funzione di Compliance a livello di Paese e non per singola società.
Il ruolo e i requisiti della funzione di Compliance sono regolati in specifiche *Global Compliance Rules* emanate da Unicredit e recepite dalle società del Gruppo, così da assicurare che questioni similari vengano gestite in modo omogeneo nell'ambito dei vari ordinamenti in cui opera il Gruppo.
Il perimetro di competenza della funzione di Compliance comprende le normative riguardanti le tematiche bancarie e finanziarie e i regolamenti Consob e Banca d'Italia. La responsabilità della Direzione non si estende alla normativa fiscale[129].

Le attività di internal auditing effettuate dalle competenti strutture delle singole società del Gruppo sono indirizzate, coordinate e supervisionate dalla funzione di Internal Audit di Unicredit, organizzata anch'essa in *Department*. In alcuni casi tali attività sono realizzate in outsourcing vero la Capogruppo sulla base di specifici contratti di service che regolano le modalità di svolgimento dell'attività.
L'*Internal Audit Department*, oltre a coordinare i controlli di Audit a livello locale, svolge attività di controllo di 3° livello anche con verifiche in loco nei confronti della Capogruppo e delle controllate, nel rispetto degli *Internal Audit Group Standards* approvati dagli organi di governo di Unicredit e delle *Linee guida di Audit di Gruppo* deliberate dal C.d.a..
La nomina e la revoca del Responsabile del *Department* è affidata al C.d.a., previo parere del *CCI&R* e sentito il Collegio Sindacale. Il Responsabile del *Department* riferisce direttamente o per il tramite del Comitato al C.d.a. e dipende gerarchicamente dallo stesso.
Il *Department* opera in conformità al "Mandato di Audit di Gruppo", documento, revisionato lo scorso 29 ottobre 2013, che ne formalizza la mission, le responsabilità, il posizionamento organizzativo, l'indipendenza, i compiti e l'autorità.
L'Internal Audit di Gruppo svolge un'indipendente ed obiettiva attività di consulenza e assurance, al fine di valutare e contribuire al miglioramento del sistema dei controlli interni del Gruppo.
I servizi di consulenza offerti hanno lo scopo di fornire supporto a Unicredit nel raggiungimento dei propri obiettivi, attraverso l'offerta di consulenza in materia di disegno, funzionamento e miglioramento del sistema dei controlli interni.
Nell'ambito dell'attività di assurance, il Responsabile del *Department Internal Audit* fornisce annualmente una valutazione circa l'adeguatezza e l'efficacia del sistema dei controlli interni del Gruppo, esaminando le evidenze riscontrate nel corso delle proprie attività di verifica.
In tale contesto il Responsabile sviluppa un *Piano di Audit* annuale da sottoporre all'approvazione del Consiglio, lo implementa, svolge investigazioni speciali richieste dal Management o dal *CCI&R* e sintetizza i risultati delle attività di Audit agli organi aziendali.
In particolare, predispone trimestralmente il report *IAAR – Internal Audit Activities and Results* che, oltre alla valutazione del sistema dei controlli interni, contiene informazioni di sintesi sull'attività svolta e sui rischi emersi, e trasmette direttamente al Collegio Sindacale e al *CCI&R* gli *Audit Report* che hanno evidenziato una valutazione critica del sistema dei controlli interni o carenze di rilevo.
La pianificazione delle attività della funzione in questione si basa sui risultati di *Risk Assessment* dell'*AU - Audit Universe* di Unicredit. La metodologia applicata è articolata, in sintesi, nelle seguenti principali fasi: definizione dell'*AU*, ossia analisi organizzativa e di

[129] Unicredit si è preoccupata di specificare all'interno della Relazione che il perimetro di competenza della funzione in questione alla data di approvazione del documento (11 marzo 2014) era in corso di aggiornamento.

processo finalizzata all'individuazione degli elementi interessati dall'attività di Audit; *Risk Assessment,* o identificazione, valutazione e graduazione dei rischi ai quali sono esposti gli elementi dell'*AU*; sulla base dei risultati dell'assessment, definizione del Piano di Audit che stabilisce obiettivi, tipologia e frequenza degli interventi di Audit.
Il Responsabile ha predisposto i *Piani di Audit di Gruppo* e il *Piano di Audit di Unicredit* come parte del *Piano Pluriennale* a 5 anni. Il Piano Pluriennale, rivisto annualmente sulla base del risk assessment, permette un'efficiente ed efficace copertura dell'*AU*. Nell'ambito dei piani menzionati sono incluse attività di IT auditing.
Nel corso del 2013, il Responsabile della funzione Internal Audit, nel rispetto delle *Linee Guida di Audit di Gruppo*, ha effettuato interventi sia sulla struttura centrale della Holding, sia sulle Subsidiaries.
Il Responsabile ha, altresì, esercitato il ruolo di indirizzo, coordinamento e controllo, regolando, coordinando e sorvegliando le attività di controllo di 3° livello svolte dalle funzioni di Audit delle società del Gruppo.
Ha inoltre proseguito nell'attività di aggiornamento degli Standards e delle policies esistenti per supportare il processo di Audit, nonché nella revisione del Mandato di Audit di Gruppo.

4.2.3 Il Group Risk Management Department

Andando a focalizzare l'attenzione sulla gestione del rischio e sulla sua governance, la funzione di Risk Management del Gruppo o *Group Risk Management Department* esercita il proprio ruolo di indirizzo, coordinamento e controllo dei rischi.
All'interno della Direzione di Risk Management svolge un ruolo chiave il *CRO – Chief Risk Officer*, situato a diretto riporto dell'Amministratore Delegato.
La Direzione presidia e controlla i rischi del Gruppo attraverso i *Portfolio Risk Managers* responsabili ciascuno per i rischi di competenza.
Il modello organizzativo prevede inoltre uno specifico punto di riferimento per l'Italia nella funzione *CRO Italy*, cui sono state assegnate responsabilità relative ai rischi del perimetro Italia e al coordinamento manageriale delle funzioni di Risk Management presso le entità italiane del Gruppo.
Al fine di rafforzare il controllo dei rischi di Gruppo sono operativi tre specifici Comitati responsabili in materia di rischi:

- *Group Risk Committee*, responsabile per le decisioni strategiche sui rischi a livello di Gruppo;
- *Group Portfolio Committees*, cui sono assegnati il compito di indirizzare, controllare e gestire i differenti rischi a livello di portafoglio; si citano, ad esempio, il Group Market Risk Committe, il Group Credit and Cross-border Risks Commitee e il Group Operational and Reputational Risks Committe;
- *Group Transactional Committees*, responsabili della valutazione di singole controparti/transazioni al di sopra di determinate soglie; si citano, tra gli altri, il Group Credit Committe e il Group Rating Committe

In particolare, il *Group Risk Commitee* ha funzioni deliberative o consultive e propositive con riferimenti a vari aspetti concernenti la governance del rischio.
Il compito di maggiore importanza riguarda la definizione del *RAF* di Gruppo, da cui deriva l'ulteriore onere di trasmettere alle entità locali gli obiettivi in termini di risk appetite, i limiti e le soglie di tolleranza. Il tema, considerata la sua rilevanza, viene approfondito nel paragrafo successivo.
La massima attenzione al risk management si evince anche dal ruolo assegnato agli stress test nella valutazione dei rischi di Unicredit. Questi vengono regolarmente applicati al portafoglio rischi del Gruppo come mezzo per stimare gli effetti sulle esposizioni della banca di scenari finanziari estremi, ma plausibili. Vengono effettuati stress test a livello di Gruppo almeno due volte l'anno.

4.2.4 Il RAF

Rispetto al RAF in essere nell'esercizio 2013, il nuovo framework per il 2014, approvato dal C.d.a. e inviato alle società del Gruppo, ha definito differenti opzioni di rischio e profittabilità all'interno del Gruppo, basate su scenari alternativi e ipotesi di stress, divenendo strumento manageriale efficace anche a fini previsionali.

Lo scopo principale della creazione di un impianto strutturato di propensione al rischio come compiuto da Unicredit è quello di assicurare che l'attività della banca si sviluppi entro i limiti di tolleranza del rischio fissati dal C.d.a.. Di conseguenza, la propensione al rischio è integrata nei processi di pianificazione strategica e di elaborazione dei budget e definita a livello di Gruppo.

Il *RAF* di Unicredit è definito dal *Group Risk Committee* a seguito di una proposta congiunta da parte delle funzioni di *Planning Finance & Administration* e *GRM*, ed esprime attraverso l'identificazione di metriche di riferimento il profilo di rischio del gruppo.

Attualmente le metriche utilizzate nel Gruppo UniCredit sono raggruppate in tre dimensioni: *Adeguatezza Patrimoniale*, *Redditività & Rischio*, *Liquidità & Funding*, compongono insieme il quadro di riferimento del risk appetite.

Le metriche di *Adeguatezza patrimoniale* sono 4:

- *Core Tier 1 Ratio* e *Total Core Ratio*, che garantiscono il bilanciamento tra capitale e rischio;
- *Leverage Ratio*, avente lo scopo di garantire la coerenza tra le dimensioni del capitale proprio e degli attivi di bilancio;
- *Risk Taking Capacity*, ossia il rapporto tra risorse finanziarie disponibili e Capitale Interno, che fornisce un'indicazione della capacità economica di assunzione dei rischi da parte del Gruppo[130].

La metrica di *Redditività & Rischio* coincide con la *Loss Absorption Capacity*. Quest'ultima definisce quanto il Gruppo possa permettersi di perdere in termini di conto economico sulla base dei rischi assunti e guida il budget attraverso la definizione dei limiti[131].

Tra le metriche di *Liquidità & Funding*, il *Cash Horizon*, lo *Structural Ratio* e il *Survival Period dello Stress Test della liquidità* sono definiti in coerenza con la Liquidity Policy del Gruppo, mentre il *Loan-Depo Gap* è funzionale all'obiettivo del Gruppo di ottimizzare struttura e costi del funding[132].

Il *RAF* di gruppo, però, non include solo la lista delle metriche rilevanti, ma anche i *target*, i *trigger* e i *limiti*. I *target* o valori obiettivo rappresentano l'ammontare di rischio che il gruppo è disposto ad assumere e a cui la Banca deve tendere per raggiungere gli obiettivi di budget, mentre i *trigger* o valori di allerta rappresentano delle soglie di allarme che attivano l'analisi di possibili azioni di mitigazione e prevedono un'informativa al *Group Risk Committee*, ed infine i *limiti* costituiscono i valori che non devono essere superati. Nel caso in cui vengano superati i limiti di riferimento, il Consiglio di Amministrazione deve esserne informato.

A seguito della definizione di metriche e di target/trigger/limiti, il risk appetite viene regolarmente monitorato e un processo di escalation ai livelli organizzativi appropriati garantisce una reazione tempestiva nel caso in cui i valori delle metriche si avvicinino o superino trigger e limiti.

[130] Cfr. Unicredit, *Risposta al documento di consultazione*, novembre 2012.
[131] *Ibid*.
[132] *Ibid.*

La definizione di strategie di rischio rappresenta un passaggio chiave dell'integrazione del *RAF* nel business ed è il modo con cui il *Group Risk Committee* comunica e incorpora target e limiti delle esposizioni di rischio nell'operatività del Gruppo.

4.3 UBI Banca

> *"Il Sistema di controllo interno [...] costituisce elemento essenziale del sistema di corporate governance di UBI Banca e delle Società del Gruppo. UBI Banca ha adottato un Sistema di controllo interno che [...] ripartisce funzioni e competenze fra diversi attori, in costante rapporto dialettico tra loro e supportati da regolari flussi informativi, che contribuiscono all'efficienza del Sistema dei controlli medesimo".*

Il processo di impostazione del sistema dei controlli del Gruppo e la verifica dell'adeguatezza e dell'effettivo funzionamento dello stesso rientrano tra i compiti assegnati agli organi con funzione di supervisione strategica, controllo e gestione di UBI Banca[133].
Intervengo a tal fine:
- il Consiglio di Sorveglianza e il Comitato per il Controllo interno;
- il Consigliere esecutivo incaricato del sistema dei controlli interni;
- le funzioni aziendali di controllo.

4.3.1 Il ruolo degli organi aziendali

Il Consiglio di Sorveglianza di UBI Banca assomma alcuni poteri che nel sistema tradizionale sono propri dell'Assemblea e del Collegio Sindacale, assumendo funzioni di alta amministrazione e controllo del Gruppo[134]. Si occupa, infatti, tra le altre cose, della nomina dei componenti del Consiglio di Gestione e dell'approvazione del bilancio d'esercizio, nonché esercita le funzioni di vigilanza previste a carico del Collegio Sindacale dall'art. 149 del TUF. Per quanto concerne nello specifico il sistema dei controlli interni, il Consiglio di Sorveglianza del Gruppo: definisce gli obiettivi di rischio; determina le politiche di assunzione, gestione e controllo dei rischi, verificandone nel continuo l'adeguatezza e l'attuazione da parte del Consiglio di Gestione; delibera in ordine alle politiche di gestione del rischio di conformità e alla costituzione della funzione di conformità alle norme; formula le proprie valutazioni in ordine alla definizione degli elementi essenziali dell'architettura complessiva del sistema dei controlli interni; valuta il grado di efficienza dello stesso; esprime il proprio parere in ordine alle nomina e revoca da parte del Consiglio di Gestione dei Responsabili della funzione di controllo interno e di conformità.

Nell'assolvimento delle proprie competenze in qualità di organo di controllo, il Consiglio di Sorveglianza si avvale dell'assistenza del *Comitato per il Controllo interno*[135] di sua diretta emanazione, che opera con funzioni istruttorie, consultive e propositive. L'attività del Comitato è disciplinata da un apposito Regolamento che ne determina i compiti e le modalità di funzionamento.

---

[133] UBI Banca ha adottato il sistema di amministrazione e controllo dualistico composto dal Consiglio di Sorveglianza, organo nominato direttamente dai soci e avente funzioni di supervisione strategica e controllo, e dal Consiglio di Gestione con funzione di gestione dell'impresa. I componenti del Consiglio di Gestione vengono nominati dal Consiglio di Sorveglianza.

[134] Il Consiglio di Sorveglianza di UBI Banca ricopre, quindi, l'importante ruolo assegnato dalla disciplina agli organi con funzione di supervisione strategica e controllo. Si veda infra par. 2.1.2.

[135] Il Comitato per il Controllo Interno rappresenta uno dei 5 comitati consiliari costituiti all'interno del Consiglio di Sorveglianza di UBI Banca con funzioni propositive, consultive e istruttorie.

Il Comitato, avvalendosi delle strutture aziendali preposte, può procedere in qualsiasi momento ad atti di ispezione e di controllo nonché scambiare informazioni con gli organi di controllo delle società del Gruppo. In particolare il Comitato, qualora ne ravvisi la necessità, chiede alla funzione di Internal Audit lo svolgimento di verifiche su ambiti specifici. Inoltre, Il Comitato attiva la funzione di Internal Audit a seguito di richieste straordinarie di intervento ispettivo e/o indagine formulate dal Consigliere Delegato.
Il Comitato riferisce periodicamente al Consiglio di Sorveglianza sull'attività svolta attraverso apposite relazioni semestrali, nell'ambito delle quali esprime anche il proprio giudizio sull'adeguatezza del sistema dei controlli interni della Banca e delle controllate aventi rilevanza strategica. Inoltre, il Presidente del Comitato segnala per tempo al Consiglio di Sorveglianza gli ambiti di miglioramento osservati richiedendo l'adozione di idonee misure di rafforzamento e verificandone nel tempo l'efficacia.
Agli incontri del Comitato partecipano stabilmente il *CRO – Chief Risk Officer* e il *CAE – Chief Audit Executive*, strutture di cui ci occuperemo nel paragrafo successivo.
Nel corso dell'esercizio 2013 il Comitato si è riunito 27 volte. Per quanto riguarda l'attività prevista per il 2014, il Comitato ha programmato lo svolgimento di 26 riunioni.

Il Consiglio di Gestione del Gruppo è costituito in prevalenza da Consiglieri esecutivi. I Consiglieri di gestione sono infatti attivamente coinvolti nella gestione della società in conformità agli indirizzi approvati dal Consiglio di Sorveglianza[136]. In particolare, il Consiglio di Gestione ha attribuito al *Consigliere Delegato* precise deleghe gestionali. Oltre al Consigliere Delegato sono assegnati al Presidente ed al Vice Presidente del Consiglio di Gestione poteri e funzioni che sottolineano il loro coinvolgimento nell'amministrazione della Banca.
Il Consiglio di gestione ha inoltre affidato al Consigliere Delegato l'incarico concernente la progettazione dell'architettura complessiva del sistema dei controlli interni. Spetta, pertanto, a questa figura l'attuazione del processo di gestione dei rischi.
Nell'ambito di tale incarico il Consigliere Delegato ha promosso l'introduzione dei "Principi per l'impostazione del Sistema di controllo Interno del Gruppo UBI", approvati nel mese di ottobre 2008. L'applicazione degli stessi è estesa a tutte le società appartenenti al Gruppo.

In conformità al 15° aggiornamento alla Circ. 263/2006, Il Consiglio di Gestione e il Consiglio di Sorveglianza del Gruppo hanno approvato, nel mese di luglio 2013, che la composizione dell'O.d.V. ex d.lgs. 231/2001 corrisponda a quella del *Comitato per il Controllo Interno.* Per le società controllate è stato, invece, stabilito che l'incarico sia conferito al Collegio Sindacale.

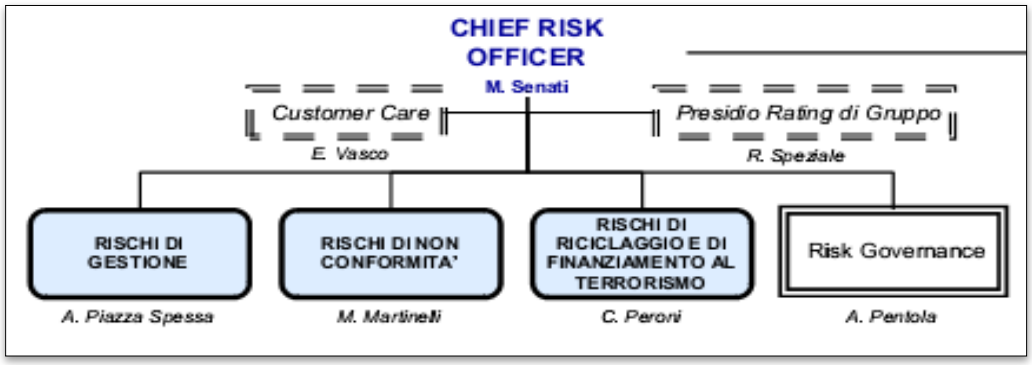
4.3.2 Il Chief Risk Officer e il Chief Audit Executive

I controlli di linea o di 1° livello di UBI Banca sono affidati ai Responsabili delle unità organizzative o di processo e risultano integrati nell'ambito dei processi di appartenenza.

Per quanto riguarda i controlli di 2° livello, la configurazione organizzativa del Gruppo, come mostrata nella Figura 3, prevede la presenza di un *CRO - Chief Risk Officer* a riporto del Consigliere Delegato, le cui strutture comprendono sotto un unico presidio le Aree *Rischi di Gestione*, *Rischi di non conformità* e *Rischi di riciclaggio e finanziamento del terrorismo* e il Servizio *Risk Governance.* Sono a diretto riporto del *CRO* anche le strutture di staff dedicate alla *Customer Care* ed al *Presidio del rating di Gruppo*.

[136] Il Consiglio di Gestione di UBI Banca ricopre, quindi, l'importante ruolo assegnato dalla disciplina all'organo con funzione di gestione. Si veda infra par. 2.1.2.

Figura 3: UBI Banca - *I controlli sui rischi*



Fonte: sito web www.ubibanca.it

Il *CRO* ha il compito di formalizzare il quadro di riferimento per la determinazione del *RAF* di Gruppo, è responsabile dell'attuazione delle politiche di governo e relative al sistema di gestione dei rischi garantendo, nell'esercizio della funzione di controllo, una vista integrata delle diverse rischiosità agli organi aziendali. Per il tramite delle attività svolte dalle proprie strutture assicura la misurazione e il controllo dell'esposizione di Gruppo alle diverse tipologie di rischio. Inoltre contribuisce allo sviluppo e alla diffusione di una cultura del controllo all'interno del Gruppo presidiando l'identificazione e il monitoraggio di eventuali disallineamenti rispetto alla normativa di riferimento.
La struttura del *CRO*[137] si articola, come anticipato e mostrato dalla figura di cui sopra, nelle seguenti unità organizzative:

- unità di staff *Custommer Care*, che supporta l'Alta Direzione nello sviluppo delle politiche aziendali volte alla diffusione di una cultura di attenzione e soddisfazione del Cliente e ricopre il ruolo di Ufficio Reclami di UBI;
- unità di staff *Presidio Rating di Gruppo*, che garantisce il presidio complessivo del rating di Gruppo, coordinandosi con le altre strutture competenti;
- area *Rischi di non Conformità*, che assicura il presidio del rischio di non conformità alle norme interne e esterne che disciplina l'attività bancaria;
- area *Rischi di Riciclaggio e di Finanziamento al Terrorismo*, che presidia le attività di contrasto al riciclaggio ed al finanziamento al terrorismo;
- area *Rischi di Gestione*, che supporta il *CRO* nelle attività di attuazione delle politiche e del processo di gestione dei rischi; l'area in questione garantisce la misurazione ed il controllo dell'esposizione di Gruppo alle diverse tipologie di rischio, sviluppando i relativi modelli di misurazione, garantendo la piena attuazione delle relative politiche di assunzione e gestione, mediante l'effettuazione dei controlli di secondo livello;
- servizio *Risk Governance*, che attraverso l'interazione con le altre strutture a riporto del *CRO*, contribuisce a garantire l'adeguatezza nel continuo del processo dei rischi, producendo la reportistica di sintesi di Gruppo per il monitoraggio integrato dei rischi correnti e prospettici e dei relativi interventi di mitigazione.

Il 3° livello dei controlli, altrimenti detto Revisione Interna, viene svolto dalla funzione di Internal Audit che fa capo al *CAE - Chief Audit Executive* alle dirette dipendenze del Consiglio di Sorveglianza.
La funzione di Interan Audit effettua attività di controllo di terzo livello su UBI Banca, sulle controllate che hanno delegato alla capogruppo lo svolgimento della funzione di revisione interna e, più in generale, sulle società del Gruppo. Relativamente a tale perimetro, l'Internal Audit controlla, anche con verifiche in loco, in coerenza con gli Standard Internazionali della

[137] UBI Banca ha ritenuto opportuno precisare nella Relazione che sono in corso valutazioni in merito alla struttura del CRO per l'adeguamento della stessa al disposto normativo dell'aggiornata Circ. 263/2006.

professione, l'operatività e l'idoneità del sistema di controllo interno e gestione dei rischi, sulla base di un Piano Pluriennale delle attività. Tale pianificazione sviluppata su un orizzonte triennale è basata sugli esiti della valutazione periodica delle rischiosità presenti nelle diverse società o nei processi di Gruppo.
Gli esiti degli interventi di audit sono oggetto, oltre che di specifica informativa rilasciata al Referente Audit e alla Direzione Generale della Società alla conclusione delle attività di analisi, di una rendicontazione periodica a favore dei C.d.a. e dei Collegi Sindacale delle controllate e cumulativamente rappresentata al Comitato per il Controllo Interno, al Consiglio di Gestione e al Consiglio di Sorveglianza della Capogruppo. In caso di eventi di particolare rilevanza la funzione predispone e trasmette agli organi aziendali di amministrazione e controllo, nonché al Consigliere esecutivo incaricato del sistema dei controlli interni, una informativa tempestiva e adeguata.

4.3.3 La tolleranza al rischio

La Relazione di UBI Banca non si sofferma sul tema del *RAF* di Gruppo. Informazioni utili possono tuttavia apprendersi nel documento pubblicato nel mese di ottobre 2012[138] che rappresenta la sintesi dei commenti e delle proposte del Gruppo sui vari argomenti trattati nel documento per la consultazione di Banca d'Italia in materia di sistema dei controlli interni, sistema informativo e continuità operativa.
Si ricavano, infatti, dalle considerazioni espresse dalla Banca, informazioni in merito alle variabili di natura quantitativa utilizzate per declinare la tolleranza al rischio, che fanno riferimento ai seguenti aspetti:

- solidità patrimoniale, espressa sia in termini di misure regolamentari (CT1) sia interne (rapporto tra risorse finanziarie disponibili – AFR – e capitale interno complessivo);
- equilibrio finanziario, espresso sia in termini di corretto equilibrio tra le fonti e gli impieghi (NSFR), sia di adeguate riserve liquide per fronteggiare situazioni di crisi (LCR);
- creazione di valore (EVA);
- valutazione del posizionamento sul mercato, basato sulla determinazione del rating target tendenziale;
- assetto organizzativo-informatico e dei controlli, basato sulla minimizzazione dei possibili impatti derivanti dai rischi perseguibile attraverso l'adozione di policy a presidio dei rischi, rigorosi presidi organizzativi, metodologie di misurazione e strumenti di mitigazione.

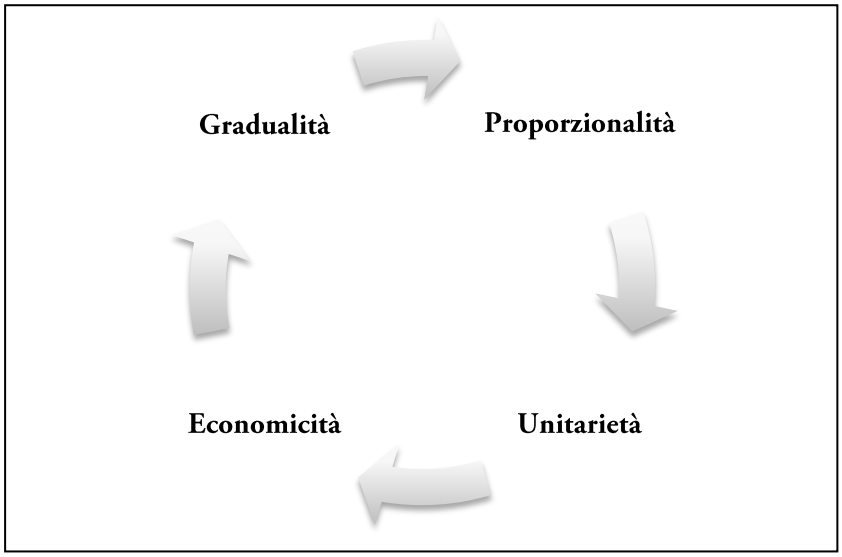
4.4 Banca Popolare di Sondrio

> *"La banca, consapevole che il Sistema dei controlli interni costituisce un elemento determinante affinché l'attività sia sempre improntata ai tradizionali criteri di "sana e prudente gestione", è impegnata con continuità in un'opera finalizzata alla razionalizzazione e all'aggiornamento del sistema stessa".*

La Banca è pervenuta ad un sistema che consente la rilevazione, misurazione e gestione di tutte le tipologie di rischio che la stessa ritiene rilevanti, in conformità a taluni principi statuiti dalla Vigilanza e mostrati in Figura 4.

[138] UBI Banca, *Considerazioni UBI Banca sul documento per la consultazione di Banca d'Italia*, ottobre 2012.

Figura 4: Banca Popolare di Sondrio – *Linee guida dell'architettura dei controlli*



Al fine di disciplinare dal punto di vista metodologico, organizzativo, operativo e informativo la gestione dei rischi che la banca assume quotidianamente, sono stati predisposti per ciascuna fattispecie di rischio due tipologie di regolamenti:

- il *Regolamento del processo*, che disciplina i criteri per la gestione dei rischi associati ai processi e il ruolo al quale sono chiamati gli organi e le unità organizzative per la realizzazione dei predetti criteri;
- il *Regolamento del procedimento operativo*, che norma le componenti necessarie all'attuazione dei citati criteri quali le attività, le procedure e le strutture organizzative.

Il sistema dei controlli del gruppo coinvolge con ruoli diversi:

- il Consiglio di Amministrazione;
- la Direzione Generale;
- il Collegio Sindacale;
- le funzioni aziendali di controllo.

4.4.1 Il ruolo degli organi di vertice

Il Consiglio di Amministrazione[139], in quanto organo con funzione di supervisione strategica, è responsabile della definizione, approvazione e revisione delle politiche di governo dei rischi. A tal fine non si avvale del supporto di un comitato competente in materia[140]. Il C.d.a. della Banca ha nominato i membri del Comitato esecutivo, tra i quali rientra il Consigliere delegato[141].

Spetta, invece, alla Direzione Generale rendere effettiva l'esecuzione delle politiche in materia di sistema dei controlli interni stabilite dall'organo con funzione di supervisione strategica[142]. Il Direttore Generale è, infatti, responsabile dell'istituzione e del mantenimento di un sistema per la governance del rischio efficace ed efficiente, coerente con gli indirizzi strategici delineati dal Consiglio di Amministrazione e dal Comitato Esecutivo.

[139] La Banca Popolare di Sondrio adotta il modello di amministrazione e controllo tradizionale.
[140] Gli unici comitati consiliari costituti sono il Comitato operazioni con parti correlate e il Comitato remunerazione.
[141] Non vi sono consiglieri esecutivi in aggiunta al Consigliere delegato e ai componenti del Comitato esecutivo.
[142] Il Direttore Generale ricopre, pertanto, l'importante ruolo assegnato dalla disciplina all'organo con funzione di gestione. Si veda infra par. 2.1.2.

Esercita, invece, le proprie responsabilità istituzionali di controllo, il Collegio Sindacale, contribuendo ad assicurare la regolarità e la legittimità della gestione[143].

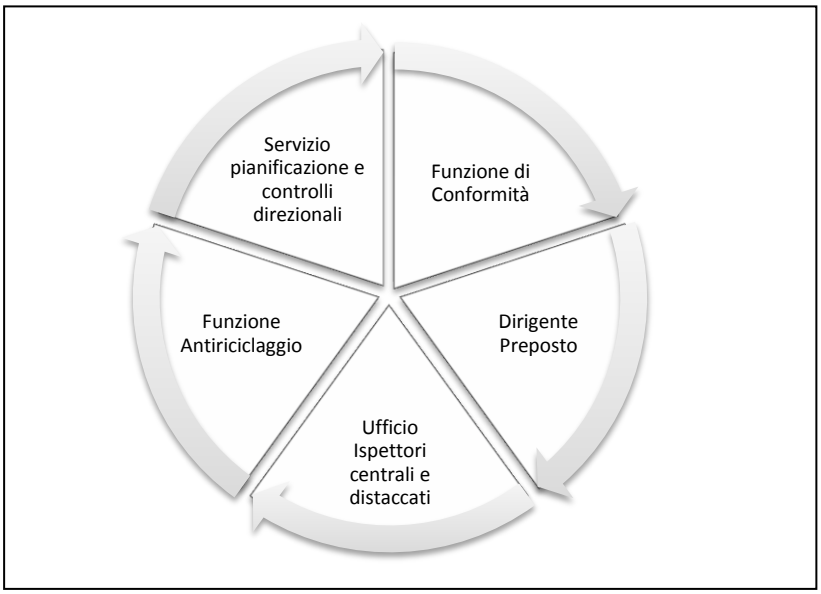
L'O.d.V. ex d.lgs. 231/2001 è composto da un Consigliere di amministrazione, dal Responsabile della Funzione di Conformità, dal Responsabile della Revisione Interna e dal Responsabile dell'ufficio legale e contenzioso.

4.4.2 Gli attori del controllo sulla gestione dei rischi e la Revisione Interna

I controlli di linea o di 1° livello del Gruppo, qualora non integrati nelle procedure informatiche, sono demandati alle stesse unità aziendali, comprese le strutture di back-office, alle quali viene attribuita la responsabilità di esecuzione dei processi o di parte di essi.

I controlli di 2° livello sono diretti a definire i criteri e le metodologie per la rilevazione e la misurazione dei rischi e a verificarne il rispetto.
Le unità organizzative della Banca alle quali sono demandati i controlli della specie, che possiamo definire controlli sulla gestione dei rischi, sono molteplici. Dopo averli rappresentati in Figura 5, passeremo ad evidenziarne i principali compiti.

Figura 5: Banca Popolare di Sondrio – *Gli attori del controllo sulla gestione dei rischi*



Il *Servizio pianificazione e controlli direzionali* ha la missione di predisporre, gestire e diffondere sistemi idonei per la misurazione e il controllo delle varie fattispecie di rischio ritenute rilevanti, nonché di presidiare la strumentazione metodologica e informativa per la realizzazione dei processi di pianificazione e controllo della gestione aziendale. In particolare:

- sviluppa le metodologie, gli strumenti e i processi per l'identificazione, la valutazione e la misurazione dei rischi connessi all'attività aziendale e produce la relativa reportistica;
- provvede a misurare e valutare in modo attendibile, tempestivo, sistematico e completo l'esposizione ai rischi;
- monitora l'esposizione del Gruppo, sia attuale che prospettica, riferita alle diverse tipologie di rischio rilevanti;
- coordina il processo di identificazione e valutazione dei rischi presenti nelle diverse attività aziendali, funzionale alla redazione del resoconto ICAAP a alla stima dell'adeguatezza patrimoniale attuale e prospettica.

[143] La Banca Popolare di Sondrio assegna, quindi, al Collegio Sindacale il ruolo attribuito dalla disciplina all'organo con funzione di controllo . Si veda infra par. 2.1.2.

- predispone il piano di sviluppo interno pluriennale e trimestralmente valuta gli scostamenti dei risultati conseguiti rispetto a quelli attesi

La *Funzione di Conformità* si occupa dei controlli relativi alla conformità dei processi e delle procedure aziendali alle norme di eteroregolamentazione e di autoregolamentazione, con lo scopo di prevenire i rischi legale e reputazionale. La Funzione è coordinata da un Responsabile ed è costituita da risorse che operano in unità organizzative interessate alle tematiche rientranti nel perimetro della compliance.
Il *Dirigente preposto* ha la missione di assicurare l'attendibilità dell'informativa contabile e finanziaria mediante la predisposizione di adeguate procedure amministrativo-contabili e il monitoraggio nel continuo circa la loro adeguatezza ed effettiva applicazione.
All'*Ufficio Ispettori centrali e distaccati*, collocato all'interno del *Servizio Revisione Interna*, compete la verifica della correttezza dei comportamenti assunti dalle unità organizzative nello svolgimento delle attività loro assegnate. Assume inoltre compiti di accertamento anche con riguardo a specifiche irregolarità o inadempienze.
La *Funzione Antiriciclaggio*, posta alle dipendenze del Direttore Generale, attua un presidio continuativo, allo scopo di prevenire e contrastare il rischio derivante dal coinvolgimento in operazioni di riciclaggio e di finanziamento del terrorismo. Valuta l'adeguatezza e l'idoneità dei pertinenti processi organizzativi e gestionali della banca rispetto alla normativa tempo per tempo vigente in materia.

I controlli di 3° livello sono demandati all'unità organizzativa costituita dalla *Revisione Interna ed EDPAuditing*, istituita funzionalmente all'interno del *Servizio Revisione Interna*.
La struttura è tenuta a verificare, sia a livello di capogruppo che a livello locale, il funzionamento del sistema dei controlli interni, formulando anche proposte di miglioramento delle procedure e delle modalità di assunzione e monitoraggio dei rischi. In particolare, le relazioni periodiche prodotte dal Servizio sono di supporto ai vertici aziendali per accertare l'adeguatezza e la funzionalità del sistema dei controlli interni e per adottare con tempestività, qualora emergano carenze o anomalie, idonee misure correttive.
Per quanto attiene alle metodologie di lavoro utilizzate, la funzione ricorre ad analisi di processo, verifiche in loco e a distanza, nonché a monitoraggi automatici per mezzo di indicatori di anomalia.

4.5 Alcune considerazioni conclusive

Le informazioni reperite permettono di confrontare la struttura dei controlli interni dei tre istituti prescelti per l'analisi. Per operare tale confronto si è ritenuto opportuno creare due distinte tabelle aventi ad oggetto rispettivamente organi aziendali e funzioni aziendali di controllo.

La Figura 6 sotto riportata fotografa gli organi aziendali che assumo responsabilità e compiti nell'ambito del sistema dei controlli interni.

In particolare si nota la presenza, all'interno del Consiglio di Amministrazione di Unicredit, del *Comitato per i Controlli Interni & Rischi*, articolato in due specifici Sotto-Comitati aventi funzioni consultive e propositive in materia di controlli interni e di rischi.
Analoghe funzioni sono svolte dal *Comitato per il Controllo Interno* di UBI Banca, istituito a supporto del Consiglio di Sorveglianza nell'assolvimento delle competenze in qualità di organo di controllo.
Per contro, il Consiglio di Amministrazione della Banca Popolare di Sondrio non ha nominato il comitato esperto in materia di controlli.

All'interno di Unicredit la progettazione e la gestione del sistema dei controlli interni spetta al *Chief Executive Officer*, supportato dal *Direttore generale* che presiede l'*Internal Control Coordination Committee*.
Analogamente, lo stesso ruolo viene svolto dal *Consigliere delegato* di UBI Banca.

Spetta, invece, al *Direttore generale* della Banca Popolare di Sondrio rendere effettiva l'esecuzione delle politiche in materia di controlli interni.

Per quanto concerne l'assegnazione delle funzioni proprie dell'O.d.V. all'organo con funzione di controllo, si segnala la presenza di un organismo appositamente istituito in Unicredit e Banca Popolare di Sondrio. Anche UBI Banca, prima del 15° aggiornamento alla Circ. 263/2006, identificava il proprio O.d.V. in un organismo collegiale. Nel corso del mese di luglio 2013 ha tuttavia preferito deliberare il conferimento dell'incarico al *Comitato per il Controllo Interno* in applicazione della nuova previsione normativa.

Figura 6: *Gli organi aziendali coinvolti nel SCI*

	UNICREDIT	**UBI BANCA**	**BANCA POPOLARE DI SONDRIO**
OFSS	***CDA*** Supportato dal ***CCI&R***, organizzato in: - Sotto-Comitato per i Controlli Interni; - Sotto-Comitato per i Rischi.	***CONSIGLIO DI SORVEGLIANZA***	***CDA***
OFG	***CEO*** Supportato dall'***ICCC***, presieduto dal *D.g*.	***CONSIGLIO DI GESTIONE*** ***Consigliere delegato*** e Comitato esecutivo	***COMITATO ESECUTIVO*** Consigliere delegato ***Direttore Generale***
OFC	***COLLEGIO SINDACALE***	***CONSIGLIO DI SORVEGLIANZA*** Supportato dal ***CCI***	***COLLEGIO SINDACALE***
ODV	**Organismo appositamente istituito**	***CCI***	**Organismo appositamente istituito**

Sul fronte delle funzioni aziendali di controllo, la Figura 7 mostra le funzioni/strutture coinvolte nel sistema dei controlli interni dei tre istituti.

Per quanto attiene al 1° livello dei controlli, Unicredit si contraddistingue per aver creato una struttura responsabile del sistema dei controlli operativi di primo livello, denominata *Internal Controls Italy*.

Nell'ambito dei controlli di 2° livello, Unicredit affida lo svolgimento dei controlli sulla conformità e sui rischi a due *Department* distinti presieduti dal *Compliance Officer* e dal *Chief Risk Officer* di Gruppo.
UBI Banca, invece, riunisce i controlli sui rischi di gestione, di non conformità e di riciclaggio, sotto l'unico presidio del *Chief Risk Officer* di Gruppo.
Infine, Banca Popolare di Sondrio demanda i controlli sulla gestione dei rischi a cinque diverse unità organizzative.

Il 3° livello dei controlli viene svolto, in Unicredit, dall'*Internal Audit Department*.
Ruolo analogo è assegnato alla funzione di Internal Audit di UBI Banca presieduta dal *Chief Audit Executive*.
Anche la Banca Popolare di Sondrio assegna i controlli di 3° livello ad una specifica unità organizzativa denominata *Revisione Interna ed EDP Auditing* istituita all'interno del *Servizio Revisione Interna*.

Figura 7: Le funzioni aziendali di controllo

	UNICREDIT	UBI BANCA	BANCA POPOLARE DI SONDRIO
1° LIVELLO	Strutture/procedure informatiche/back office ***Internal Controls Italy***	Strutture operative/procedure informatiche/back office	Strutture operative/procedure informatiche/back office
2° LIVELLO	***Department Global Compliance - GCO*** ***Group Risk Management Department – GCRO*** -Portfolio Risk Managers -CRO Italy -Group Committees	***CRO*** -Rischi di Gestione -Rischi di non Conformità -Rischi di riciclaggio -Risk governance -Customer Care -Presidio Rating di Gruppo	***Controlli gestione rischi*** -Servizio pianificazione e controlli direzionali -Funzione di Conformità -Dirigente Preposto -Ufficio Ispettori centrali e distaccati (Servzio IA) -Funzione Antiriciclaggio
3° LIVELLO	***Department Internal Audit - Responsabile***	***Internal Audit - CAE***	***Revisione Interna ed EDP Auditing (Servizio IA)***

Certamente Unicredit presenta un sistema dei controlli interni saldamente articolato, regolamentato e organizzato. Sia per quanto riguarda gli organi, sia con riferimento ai tre livelli di controllo interno, il Gruppo si è dotato un'architettura a tratti complessa ma sicuramente pensata per guidare e presidiare un modello di business ricco e diversificato.

UBI Banca regge il confronto sotto il profilo degli organi aziendali coinvolti nel sistema dei controlli interni, mentre appare meno organizzata sul piano dei tre livelli del controllo interno.
La presenza di un *CRO* le cui strutture comprendono sotto un unico presidio le funzioni di Risk Management, Compliance e Antiriciclaggio è, infatti, in contrasto con quanto chiarito in merito dalla Banca d'Italia all'interno del *Resoconto della consultazione*[144].

Banca Popolare di Sondrio appare, senza dubbio, l'istituto più arretrato sul fronte dei controlli. Tra gli altri, l'assegnazione al Direttore Generale dei compiti in materia di controlli interni propri dell'organo con funzione di gestione disattende il divieto più volte ribadito dall'Autorità di Vigilanza[145].

[144] Vedi infra par. 3.1.2.
[145] Vedi infra par. 2.1.2.

Conclusioni

L'aggiornamento normativo oggetto della trattazione giunta alle conclusioni definisce il nuovo quadro di insieme in cui sono compresi ruoli e responsabilità degli organi aziendali, attività e requisiti delle funzioni aziendali di controllo, flussi informativi e relazioni tra gli attori della governance del rischio.

Oggi, pertanto tutte le banche sono chiamate a rivedere i propri modelli di gestione del rischio, verificandone l'effettiva rispondenza alle norme di legge attraverso una progressiva opera di autovalutazione e adozione di correttivi laddove necessario. Parte di tale opera di revisione è stata già condotta dagli istituti bancari italiani nell'ambito dell'adempimento di gap analysis imposto agli stessi dalla Banca d'Italia con scadenza 31 gennaio 2014.

Il piano di adeguamento alla nuova normativa, definito e approvate dalle banche in conseguenza alla gap analysis condotta, è sicuramente senza precedenti in termini di complessità, onerosità e rispetto delle scadenze imposte.
La difficoltà che lo contraddistingue è emersa anche dalle molteplici richieste di chiarimento avanzate dal sistema bancario che hanno condotto la Banca d'Italia a fornire le proprie indicazioni nell'ambito del Resoconto della consultazione e della Nota di chiarimenti del gennaio 2014, aggiornata nel mese di giugno alla luce delle persistenti difficoltà di interpretazione delle Disposizioni.
Si denota, tuttavia, nei chiarimenti forniti al sistema, una posizione dell'Autorità di Vigilanza sostanzialmente rigida, fermo restando l'applicazione del principio di proporzionalità.

Posto il fisiologico smarrimento che ha caratterizzato senza ombra di dubbio il periodo successivo alla pubblicazione della nuova normativa, le banche avrebbero dovuto cogliere la straordinaria opportunità offerta dalle Disposizioni. Probabilmente, laddove queste ultime sono state accolte con fastidio non sono ancora stati superati quei retaggi culturali ormai sorpassati e deleteri che da troppi anni condizionano e ostacolano un governo sano e prudente.

In ogni caso, l'adeguamento alla nuova normativa impegnerà seriamente tutti gli istituti bancari nazionali per oltre un biennio, richiedendo lo stanziamento di un elevato volume di investimenti in termini monetari e di risorse. Tuttavia, gli istituti che sapranno riconoscere e sceglieranno di sfruttare il valore aggiunto che l'attuazione delle Disposizioni determina, in termini di razionalizzazione, efficienza ed efficacia del governo aziendale, potranno godere nel tempo dei benefici tali da ripagare per buona parte gli sforzi condotti.

La razionalizzazione dei compiti, dei ruoli e delle responsabilità sul governo e sul controllo aziendale, merita, quindi, di essere considerata valore aggiunto con notevoli potenzialità in termini di trasparenza, efficacia e ottimizzazione dei processi e dei servizi, sia di gestione interna che di business verso la clientela.

Altrettanto importanti saranno i risultati che le banche potranno ottenere in termini di fiducia e consenso riscossi tra il pubblico dei risparmiatori e degli investitori istituzionali.

Bibliografia

ASSOCIAZIONE BANCARIA ITALIANA, *Disposizioni Banca d'Italia. Nuovo sistema dei controlli interni. Riflessioni sul capitolo VII per la Gap Analysis*, Roma, 30 ottobre 2013.

ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA, *Osservazioni dell'Associazione dei Componenti degli Organismi di Vigilanza ex D. Lgs. 231/2001 in relazione al ruolo dell'Organismo di Vigilanza*, Milano, 31 ottobre 2012.

BANCA D'ITALIA, *Istruzioni di vigilanza per le banche*, Circ. n. 229 del 21/4/1999.

BANCA D'ITALIA, *Nuove disposizioni di vigilanza prudenziale per le banche*, Circ. n. 263 del 27/12/2006.

BANCA D'ITALIA, *Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, 4 marzo 2008.

BANCA D'ITALIA, *Nota di chiarimenti in materia di governance*, 19 febbraio 2009.

BANCA D'ITALIA, *Applicazione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*, 11 gennaio 2012.

BANCA D'ITALIA, *Documento per la consultazione. Disposizioni di vigilanza prudenziale per le banche. Sistema dei controlli interni, sistema informativo e continuità operativa*, 4 settembre 2012.

BANCA D'ITALIA, *Disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni, sistema informativo e continuità operativa. Relazione sull'analisi d'impatto*, giugno 2013.

BANCA D'ITALIA, *Bollettino di vigilanza n. 7*, luglio 2013.

BANCA D'ITALIA, *Sintesi per gli utenti. Nuove disposizioni di vigilanza prudenziale per le banche (Circ. n. 263 del 27 dicembre 2006) - 15° aggiornamento sistema dei controlli interni, sistema informativo e continuità operativa*, 24 gennaio 2014.

BANCA D'ITALIA, *Il sistema dei controlli interni, il sistema informativo e la continuità operativa. Nota di chiarimenti*, 24 gennaio 2014 aggiornata il 6 giugno 2014.

COLA C., *Le novità per la funzione di compliance e la gestione ed il controllo del rischio fiscale*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

COMMITTEE OF EUROPEAN BANKING SUPERVISORS, *Guidelines on outsourcing*, 14 dicembre 2006.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, *Internal Control. Integrated Framework*, New York, dicembre 1992.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, *Enterprise Risk Management. Integrated Framework: Executive Summary and Framework*, New York, settembre 2004.

COMITATO DI BASILEA, *Schema per i sistemi di controllo interno nelle organizzazioni bancarie*, Basilea, settembre 1998.

COMITATO DI BASILEA, *Compliance and the compliance function in banks*, Basilea, aprile 2005.

DELLAROSA E., RAZZANTE R., *Il nuovo sistema dei controlli interni della banca*, Milano, Franco Angeli, 2010.

EUROPEAN BANKING AUTHORITY, *Guidelines on Internal Governance*, settembre 2011.

FERRANDO M., *Banche, italiane fuori dal podio nella classifica della governance*, Il Sole 24 ORE, 11 dicembre 2013.

FINANCIAL STABILITY BOARD, *Thematic Review on Risk Governance*, 12 febbraio 2013.

FINANCIAL STABILITY BOARD, *Principles for An Effective Risk Appetite Framework*, 18 novembre 2013.

FUMAGALLI M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

INSTITUTE OF INTERNAL AUDITORS, *Standard for the professional practice of Internal Auditing*, Florida, 2004.

MARANGONI M., *Il provvedimento di Banca d'Italia sul sistema dei controlli interni, impatti e novità*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

METELLI F., *FSB: Principles for An Effective Risk Appetite Framework*, articolo tratto dal sito www.aifirm.it.

METELLI F., *Il sistema di controllo e governo dei rischi. Le novità in materia di Risk Appetite Framework, il ruolo di organi e funzioni aziendali*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

PRIORI M., GUGLIELMETTI R., *Gli assetti di governo e controllo delle banche: la circolare di Banca d'Italia*, in Osservatorio di diritto bancario del Sole 24 ORE, 11 ottobre 2013.

PRIORI M., GUGLIELMETTI R., *Sistema dei controlli interni: l'organo con funzione di supervisione strategica*, in Osservatorio di diritto bancario del Sole 24 ORE, 23 ottobre 2013.

PRIORI M., GUGLIELMETTI R., *Istituzione e nomina delle funzioni di controllo*, in Osservatorio di diritto bancario del Sole 24 ORE, 19 novembre 2013.

QUASSO F., *L'Internal Audit alla luce delle nuove disposizioni di Vigilanza. Novità ed opportunità*, intervento al Convegno Unione Fiduciaria S.p.a., "Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controllo interni, sistemi informativi e continuità operativa", Milano, 1 ottobre 2013.

SOTTORIVA C., *Collegio sindacale e sistema dei controlli interni nell'ambito delle aziende di credito alla luce delle nuove disposizioni di vigilanza prudenziale (Banca d'Italia 2 luglio 2013) e della Direttiva 2013/36/UE*, in Rivista di Diritto Bancario, n. 12/2013.

TARANTOLA A. M., *Il sistema dei controlli interni nella governance bancaria*, intervento al Convegno DEXIA Crediop 4° Incontro Compliance, "Il sistema dei controlli aziendali: alla ricerca di una governance", Roma, 6 giugno 2008.

UNICREDIT, *Risposta al documento di consultazione*, novembre 2012.

UBI BANCA, *Considerazioni UBI Banca sul documento per la consultazione di Banca d'Italia*, ottobre 2012.